

# NETGEAR®

## N150 Wireless ADSL2+ Modem Router DGN1000Bv3

### User Manual



August 2013  
202-11326-01

350 East Plumeria Drive  
San Jose, CA 95134  
USA

## Support

Thank you for selecting NETGEAR products.

After installing your device, locate the serial number on the label of your product and use it to register your product at <https://my.netgear.com>. You must register your product before you can use NETGEAR telephone support. NETGEAR recommends registering your product through the NETGEAR website. For product updates and web support, visit <http://support.netgear.com>.

Phone (US & Canada only): 1-888-NETGEAR.

Phone (Other Countries): Check the list of phone numbers at <http://support.netgear.com/general/contact/default.aspx>.

## Trademarks

NETGEAR, the NETGEAR logo, and Connect with Innovation are trademarks and/or registered trademarks of NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Information is subject to change without notice. © NETGEAR, Inc. All rights reserved.

# Contents

## Chapter 1 Hardware Setup

Unpack Your Modem Router . . . . .	8
Hardware Features . . . . .	9
Front Panel . . . . .	9
Back Panel . . . . .	11
Side Panel with Restore Factory Settings Button . . . . .	12
Bottom Panel . . . . .	13
Position Your Modem Router . . . . .	13
Plug-to-WAN Jack Adapter and ADSL Microfilters . . . . .	14
German Plug-to-WAN Jack Adapter . . . . .	14
ADSL Microfilters . . . . .	14
Summary . . . . .	15
Cable Your Modem Router . . . . .	15

## Chapter 2 Getting Started

Modem Router Setup Preparation . . . . .	17
Use Standard TCP/IP Properties for DHCP . . . . .	17
Gather ISP Information . . . . .	17
Wireless Devices and Security Settings . . . . .	17
Types of Logins and Access . . . . .	17
NETGEAR genie Setup . . . . .	18
Use NETGEAR genie after Installation . . . . .	19
Update the Firmware . . . . .	19
Dashboard (BASIC Home Screen) . . . . .	20
Join Your Wireless Network . . . . .	21
Manual Method . . . . .	21
Wi-Fi Protected Setup Method . . . . .	21
NETGEAR genie App and Mobile genie App . . . . .	22

## Chapter 3 NETGEAR genie Basic Settings

Internet Setup . . . . .	24
Internet Setup Screen Fields: No Login Required . . . . .	25
Internet Setup Screen Fields: Login Required . . . . .	26
Internet Setup Screen Fields: Fields That Display Irrespective of Whether Login Is Required . . . . .	30
xDSL Setup . . . . .	30
Configure Regular Internet Service . . . . .	31
Configure IPTV Service . . . . .	32
Parental Controls . . . . .	34

Basic Wireless Settings	36
Wireless Settings Screen Fields	38
Security Options: WPA-PSK, WPA2-PSK, and WPA-PSK + WPA2-PSK Mixed Mode	39
Security Options: WPA/WPA2 Enterprise	40
Security Options: WEP	41
Set Up a Guest Network	43
View Attached Devices	44

## Chapter 4 NETGEAR genie ADVANCED Home

NETGEAR genie ADVANCED Home Screen	47
Internet Connection Setup Wizard	47
Setup Menu	48
WAN Setup	49
Default DMZ Server	51
Change the MTU Size	51
LAN Setup	53
LAN Setup Screen Settings	54
Specify DHCP Server Settings	55
Set Up Address Reservation	56
WPS Wizard for WiFi Connections	57
QoS Setup	59
WMM QoS for Wireless Multimedia Applications	59
Quality of Service Priority Rules and Internet Access	60
Bandwidth Control	67

## Chapter 5 Security

Keyword Blocking of HTTP Traffic	69
Set Up Firewall Rules to Control Network Access	70
Manage Outbound Firewall Rules	71
Manage Inbound Firewall Rules	74
Add Custom Services to Allow or Block	74
Schedule When to Block the Internet	76
Security Event Email Notifications	77

## Chapter 6 Administration

Update the Modem Router Firmware	80
View Router Status	82
Router Information	83
Internet Port	83
Modem	85
Wireless Settings	87
Guest Network	87
View and Manage the Logs	87
Change Which Actions and Events Are Logged	89
Set Up How the System Logs Are Sent	90

Manage the Configuration File . . . . .	90
Back Up Settings . . . . .	90
Restore Configuration Settings . . . . .	91
Erase the Current Configuration Settings . . . . .	91
Change the Password . . . . .	91
Password Recovery . . . . .	92
Perform Diagnostics . . . . .	93

## Chapter 7 Advanced Settings

Advanced Wireless Settings . . . . .	97
Control the Wireless Radio . . . . .	97
Set Up a Wireless Schedule . . . . .	98
View or Change WPS Settings . . . . .	100
Set Up a Wireless Access List by MAC Address . . . . .	101
Wireless Distribution System . . . . .	103
Set Up the Base Station . . . . .	104
Set Up a Repeater . . . . .	105
Port Forwarding and Port Triggering . . . . .	107
Remote Computer Access Basics . . . . .	107
Port Triggering to Open Incoming Ports . . . . .	108
Port Forwarding to Permit External Host Communications . . . . .	109
How Port Forwarding Differs from Port Triggering . . . . .	110
Set Up Port Forwarding to Local Servers . . . . .	111
Manage Custom Services for Port Forwarding . . . . .	112
Application Example: Make a Local Web Server Public . . . . .	114
Set Up and Manage Port Triggering . . . . .	114
Manage Port Triggering . . . . .	115
Manage Port Triggering Services . . . . .	116
Dynamic DNS . . . . .	118
Static Routes . . . . .	119
Remote Management . . . . .	121
Universal Plug and Play . . . . .	122
IPv6 . . . . .	123
Requirements for Entering IPv6 Addresses . . . . .	124
IPv6 Filtering . . . . .	124
Auto Detect . . . . .	124
IPv6 Auto Config . . . . .	126
IPv6 6to4 Tunnel . . . . .	127
IPv6 Pass Through . . . . .	129
IPv6 Fixed . . . . .	129
IPv6 DHCP . . . . .	131
IPv6 PPPoE . . . . .	132
Traffic Meter . . . . .	134
Restricting Internet Traffic by Volume . . . . .	136
Restricting Internet Traffic by Connection Time . . . . .	137

## Chapter 8 Troubleshooting

Quick Tips .....	139
Sequence to Restart Your Network .....	139
Check Ethernet Cable Connections .....	139
Wireless Settings .....	139
Network Settings .....	139
Troubleshoot with the LEDs .....	140
Power LED Is Off .....	140
Power LED Is Red .....	140
Power LED Is Blinking .....	141
WiFi LED Is Off .....	141
LAN LED Is Off .....	141
Cannot Log In to the Modem Router .....	141
Troubleshoot the Internet Connection .....	142
ADSL Link .....	142
Internet LED Is Red .....	143
Obtaining an Internet IP Address .....	143
Troubleshoot PPPoE or PPPoA .....	144
Troubleshoot Internet Browsing .....	144
Changes Not Saved .....	145
Wireless Connectivity .....	145
Incorrect Date or Time .....	146
TCP/IP Network Not Responding .....	146
Test the LAN Path to Your Modem Router .....	146
Test the Path from Your Computer to a Remote Device .....	147

## Appendix A Supplemental Information

Factory Settings .....	149
Technical and Physical Specifications .....	151

## Appendix B Notification of Compliance

# Hardware Setup

---

# 1

## Get to know your modem router

The NETGEAR® N150 Wireless ADSL2+ Modem Router DGN1000Bv3, going forward in this manual referred to as the modem router, provides an easy and secure way to set up a wireless home network with fast access to the Internet. You must connect the modem router to a high-speed digital subscriber line (DSL).

If you have not already set up your new modem router using the installation guide that comes in the box, this chapter walks you through the hardware setup. *Chapter 2, Getting Started*, explains how to set up your Internet connection.

This chapter contains the following sections:

- *Unpack Your Modem Router*
- *Hardware Features*
- *Position Your Modem Router*
- *Plug-to-WAN Jack Adapter and ADSL Microfilters*
- *Cable Your Modem Router*

---

**Note:** For more information about the topics covered in this manual, visit the support website at [support.netgear.com](http://support.netgear.com).

---

---

**Note:** Firmware updates with new features and bug fixes are made available from time to time on [downloadcenter.netgear.com](http://downloadcenter.netgear.com). Some products can regularly check the site and download new firmware, or you can check for and download new firmware manually. If the features or behavior of your product do not match what is described in this guide, you might need to update your firmware.

---

## Unpack Your Modem Router

Your box contains the items that are shown in the following figure. An installation guide and documentation CD are also included. In the unlikely event that any parts are incorrect, missing, or damaged, contact your NETGEAR dealer.



Figure 1. Package contents



## Hardware Features

Before you cable your modem router, take a moment to become familiar with the front panel, back panel, and label. Pay particular attention to the LEDs on the front panel.

### Front Panel

The modem router front panel has the status LEDs that are shown in the following figure. The WiFi and WPS buttons are to the left of the WiFi and WPS status LEDs.

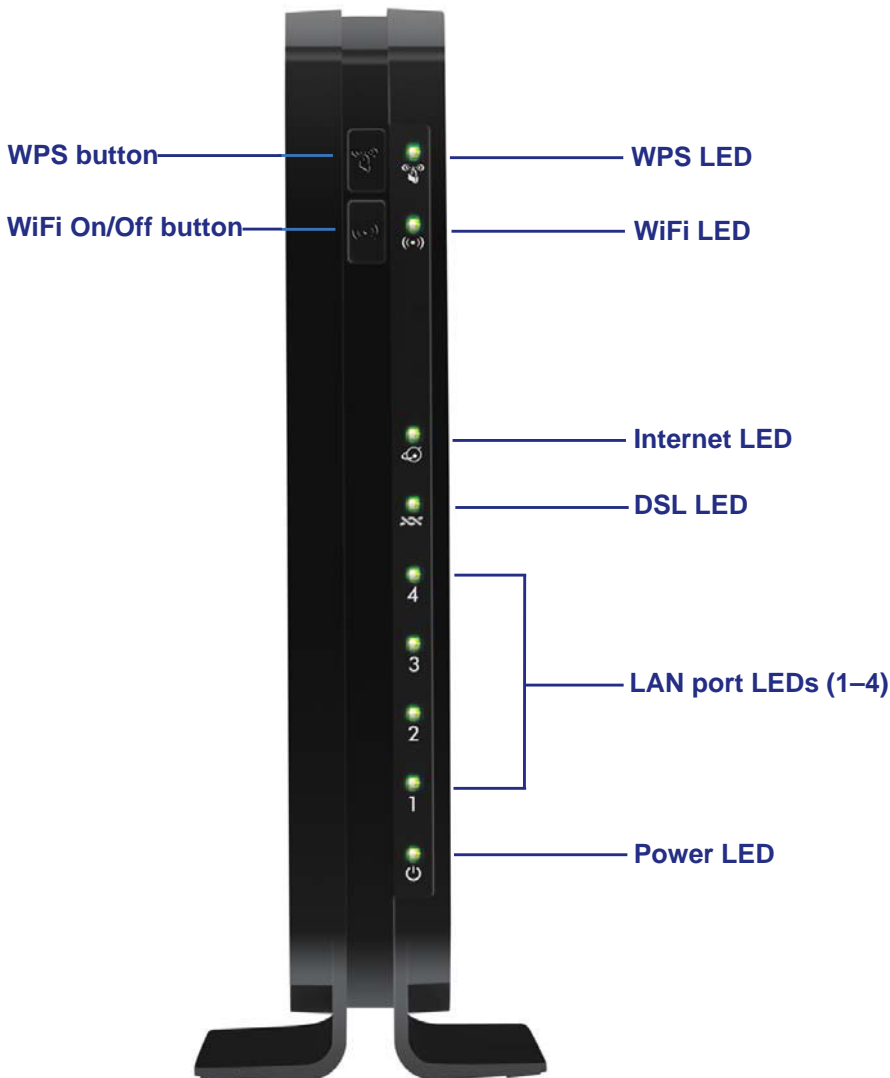










Figure 2. Front panel LEDs and buttons

The following table describes the buttons and LEDs on the front panel.

**Table 1. Front panel buttons and LEDs**

Button	LED	Description
<b>WPS</b>		Pressing the WPS button lets you use Wi-Fi Protected Setup (WPS) to join the network (see <a href="#">Wi-Fi Protected Setup Method</a> on page 21). The WPS LED has the following behavior: <ul style="list-style-type: none"> <li>• <b>Solid green.</b> Wireless security has been enabled.</li> <li>• <b>Blinking green.</b> A WPS-capable device is connecting to the device.</li> <li>• <b>Off.</b> WPS is not enabled.</li> </ul>
		
<b>WiFi</b>		Pressing the WiFi button turns the wireless radio in the modem router on or off. By default, WiFi is on. The WiFi LED has the following behavior: <ul style="list-style-type: none"> <li>• <b>Solid green.</b> There is WiFi connectivity.</li> <li>• <b>Blinking green.</b> Data is being transmitted or received over the WiFi link.</li> <li>• <b>Off.</b> There is no WiFi connectivity. You can still plug an Ethernet cable into one of the LAN ports to get wired connectivity. For more information about the use of this button, see <a href="#">Advanced Wireless Settings</a> on page 97.</li> </ul>
		
	<b>Internet</b>	<ul style="list-style-type: none"> <li>• <b>Solid green.</b> You have an Internet connection. If the connection timed out based on the setting you entered on the Internet Setup screen, but the DSL connection is still present, the LED stays green. If the Internet connection is dropped for any other reason, the LED turns off.</li> <li>• <b>Solid red.</b> The Internet (IP) connection failed. For troubleshooting information, see <a href="#">Troubleshoot the Internet Connection</a> on page 142.</li> <li>• <b>Blinking green.</b> Data is being transmitted over the DSL port.</li> <li>• <b>Off.</b> No Internet connection is detected or the device is in bridge mode (an external device handles the ISP connection).</li> </ul>
		
	<b>DSL</b>	<ul style="list-style-type: none"> <li>• <b>Solid green.</b> You have a DSL connection. In technical terms, the DSL port is synchronized with an ISP's network-access device.</li> <li>• <b>Blinking green.</b> The modem router is negotiating the best possible speed on the DSL line.</li> <li>• <b>Solid red.</b> The DSL connection is not established.</li> <li>• <b>Off.</b> The unit is off or there is no DSL link established.</li> </ul>
		
	<b>LAN (1-4)</b>	<ul style="list-style-type: none"> <li>• <b>Solid green.</b> The LAN port has detected an Ethernet link with a device.</li> <li>• <b>Off.</b> No link is detected on this port.</li> </ul>
		
	<b>Power</b>	<ul style="list-style-type: none"> <li>• <b>Solid green.</b> Power is supplied to the modem router.</li> <li>• <b>Solid red.</b> The modem router performs a power-on self-test (POST) when it starts. After about one minute, the Power LED turns solid green. If the Power LED remains red or lights red at any other time, a device malfunction has occurred.</li> <li>• <b>Off.</b> Power is not supplied to the modem router.</li> <li>• <b>Blinking red.</b> If you press the Restore Factory Settings button for seven seconds (pressing it briefly only resets the unit), the Power LED blinks red three times and then turns green as the modem router resets to the factory defaults.</li> </ul>
		

## Back Panel

The back panel has the buttons and port connections as shown in the following figure.

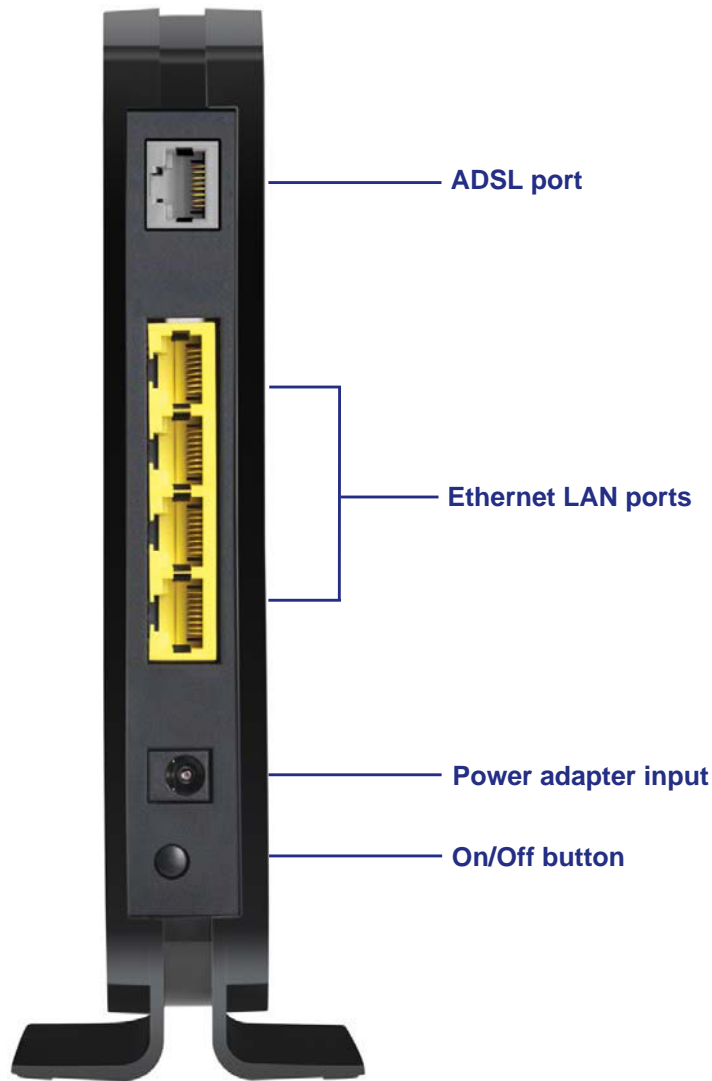


Figure 3. Back panel connections and buttons

## Side Panel with Restore Factory Settings Button

You can return the modem router to its factory settings. On the right panel of the modem router, use the end of a paper clip or some other similar object to press and hold the **Restore Factory Settings** button for at least seven seconds. The modem router resets and returns to the factory settings.



Figure 4. Right side panel with Restore Factory Settings button

For a list of factory default settings, see [Factory Settings](#) on page 149.

## Bottom Panel

The label on the bottom panel of the modem router shows the preset login information, MAC address, and serial number.

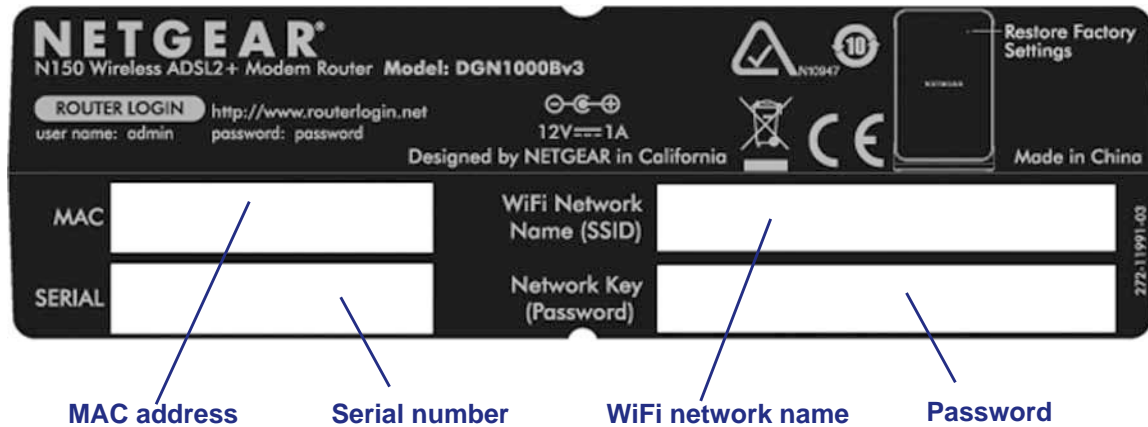


Figure 5. Label on the bottom panel of the modem router

## Position Your Modem Router

The modem router lets you access your network from virtually anywhere within the operating range of your wireless network. However, the operating distance or range of your wireless connection can vary significantly depending on the physical placement of your modem router. For example, the thickness and number of walls the wireless signal passes through can limit the range. For best results, place your modem router:

- Near the center of the area where your computers and other devices operate and preferably within line of sight to your wireless devices.
- So it is accessible to an AC power outlet and near Ethernet cables for wired computers.
- In an elevated location such as a high shelf, keeping the number of walls and ceilings between the modem router and your other devices to a minimum.
- Away from electrical devices that are potential sources of interference, such as ceiling fans, home security systems, microwaves, computers, or a 2.4 GHz cordless phone and its base.
- Away from any large metal surfaces, such as a solid metal door or aluminum studs. Large expanses of other materials such as glass, insulated walls, fish tanks, mirrors, brick, and concrete can also affect your wireless signal.

## Plug-to-WAN Jack Adapter and ADSL Microfilters

If this is the first time you have cabled a modem router between a DSL phone line and your computer or laptop, you might not be familiar with ADSL microfilters. If you are, you can skip this section and proceed to *Cable Your Modem Router* on page 15.

### German Plug-to-WAN Jack Adapter

If your subscriber line supports ADSL2+ Annex J, use the German plug-to-WAN jack adapter in between the DSL line and the microfilter or splitter. This adapter is part of the package that came with your modem router.

Plugs into the DSL line

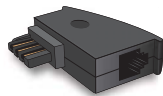


Figure 6. German plug-to-WAN jack adapter

### ADSL Microfilters

An ADSL microfilter is a small inline device that filters DSL interference out of standard phone equipment that shares the same line with your DSL service. Every telephone device that connects to a telephone line that provides DSL service needs an ADSL microfilter to filter out the DSL interference. Examples of devices are telephones, fax machines, answering machines, and caller ID displays. Not every phone line in your home necessarily carries DSL service. That depends on the DSL service setup in your home.

#### One-Line ADSL Microfilter

Plug the ADSL microfilter into the wall outlet and plug your phone equipment into the jack labeled Phone. The modem router plugs directly into a separate DSL line. Plugging the modem router into the phone jack blocks the Internet connection.



Plugs into DSL line

Figure 7. One-line ADSL microfilter

If you do not have a separate DSL line for the modem router, the best solution is to use an ADSL microfilter with a built-in splitter (see the next section, *Two-Line ADSL Microfilter*).

If you do not have a separate DSL line for the modem router, the second-best solution is to get a separate splitter. To use a one-line filter with a separate splitter, insert the splitter into the phone outlet, connect the one-line filter to the splitter, and connect the phone to the filter.

## Two-Line ADSL Microfilter

Use an ADSL microfilter with a built-in splitter if you have a single wall outlet that provides connectivity for both the modem router and your telephone equipment. Plug the ADSL microfilter into the wall outlet, plug your phone equipment into the jack labeled Phone, and plug the modem router into the jack labeled ADSL.



Figure 8. Two-line ADSL microfilter with built-in splitter

## Summary

- **German plug-to-WAN jack adapter.** Use if your subscriber line supports ADSL2+ Annex J to provide a connection between the DSL line and the microfilter or splitter.
- **One-line ADSL microfilter.** Use with a phone or fax machine.
- **Splitter.** Use with a one-line ADSL microfilter to share an outlet with a phone and the modem router.
- **Two-line ADSL microfilter with built-in splitter.** Use to share an outlet with a phone and the modem router.

## Cable Your Modem Router

Use a DSL Internet connection. For help with installation, see the installation guide that came in the package with your product and that is available online from [downloadcenter.netgear.com](http://downloadcenter.netgear.com).

For information about how to access the modem router to view or change the settings, see [Chapter 2, Getting Started](#).

## 2. Getting Started

---

# 2

### Connect to the modem router

This chapter explains how to use NETGEAR genie® to set up your modem router after you complete cabling as described in the installation guide and in the previous chapter.

This chapter contains the following sections:

- *Modem Router Setup Preparation*
- *Types of Logins and Access*
- *NETGEAR genie Setup*
- *Use NETGEAR genie after Installation*
- *Update the Firmware*
- *Dashboard (BASIC Home Screen)*
- *Join Your Wireless Network*
- *NETGEAR genie App and Mobile genie App*



## Modem Router Setup Preparation

You can set up your modem router with the NETGEAR genie automatically, or you can use the genie menus and screens to set up your modem router manually. Before you start the setup process, get your ISP information and make sure the computers and devices in the network have the settings described here.

### Use Standard TCP/IP Properties for DHCP

If you set up your computer to use a static IP address, you must change the settings so that it uses Dynamic Host Configuration Protocol (DHCP).

### Gather ISP Information

If you have DSL broadband service, you might need the following information to set up your modem router and to check that your Internet configuration is correct. Your Internet service provider (ISP) provided you with all of the information needed to connect to the Internet. If you cannot locate this information, ask your ISP to provide it. When your Internet connection is working, you no longer need to launch the ISP's login program on your computer to access the Internet. When you start an Internet application, your modem router automatically logs you in. Make sure that you have the following information:

- The ISP configuration information for your DSL account
- ISP login name and password
- Fixed or static IP address settings (special deployment by ISP; this is rare)

### Wireless Devices and Security Settings

Make sure that the wireless device or computer that you are using supports WPA or WPA2 wireless security, which is the wireless security supported by the modem router.

## Types of Logins and Access

There are separate types of logins that have different purposes. It is important that you understand the difference so that you know which login to use when.

- **Modem Router login** logs you in to the modem router web management interface. For more information about this login, see *Use NETGEAR genie after Installation* on page 19.
- **ISP login** logs you in to your Internet service. Your service provider has provided you with this login information in a letter or some other way. If you cannot find this login information, contact your service provider.
- **Wireless network key or password.** Your modem router is preset with a unique wireless network name (SSID) and password for wireless access. This information is on the label of your modem router.

## NETGEAR genie Setup

NETGEAR genie runs on any device with a web browser.

➤ **To use NETGEAR genie to set up your modem router:**

1. Turn on the modem router by pressing the **On/Off** button.
2. Make sure that your computer or wireless device is connected to the modem router with an Ethernet cable (wired) or wirelessly with the preset security settings listed on the product label.
3. Launch your Internet browser.
  - The first time you set up the Internet connection for your modem router, the browser goes to <http://www.routerlogin.net>, and the NETGEAR genie screen displays.



- If you already used the NETGEAR genie, type **<http://www.routerlogin.net>** in the address field for your browser to display the NETGEAR genie screen. See *Use NETGEAR genie after Installation* on page 19.
4. Follow the onscreen instructions to complete NETGEAR genie setup.  
NETGEAR genie guides you through connecting the modem router to the Internet.

**If the browser cannot display the web page:**

- Make sure that the computer is connected to one of the four LAN Ethernet ports or wirelessly to the modem router.
- Make sure that the modem router Power LED is solid green and the WiFi LED is lit.
- Close and reopen the browser or clear the browser cache.
- Browse to **<http://www.routerlogin.net>**.
- If the computer is set to a static or fixed IP address (this is uncommon), change it to obtain an IP address automatically from the modem router.

**If the modem router does not connect to the Internet:**

1. Review your settings to be sure that you have selected the correct options and typed everything correctly.
2. Contact your ISP to verify that you have the correct configuration information.
3. Read *Chapter 8, Troubleshooting*. If problems persist, register your NETGEAR product and contact NETGEAR technical support.

## Use NETGEAR genie after Installation

When you first set up your modem router, NETGEAR genie automatically starts when you launch an Internet browser on a computer that is connected to the modem router. If you want to view or change settings for the modem router, you can use genie again.

➤ **To access genie:**

1. Launch your browser from a computer or wireless device that is connected to the modem router.
2. Type **http://www.routerlogin.net** or **http://www.routerlogin.com**.

The login screen displays.

3. Enter **admin** for the modem router user name and **password** for the modem router password, both in lowercase letters.

**Note:** *The modem router user name and password are different from the user name and password for logging in to your Internet connection. For more information, see [Types of Logins and Access](#) on page 17.*

## Update the Firmware

When you set up your modem router and are connected to the Internet, the modem router automatically checks for you to see if newer firmware is available. If it is, a message is displayed on the top of the screen.

➤ **To update the firmware:**

1. Click the message that tells you new firmware is available.  
During the firmware update, you cannot access the Internet.
2. Click the **Yes** button to update the modem router with the latest firmware.



**CAUTION:**

To avoid the risk of corrupting the firmware, do not interrupt the update. For example, do not close the browser, click a link, or load a new page. Do not turn off the modem router.

After the update, the modem router restarts.

For more information, see [Update the Modem Router Firmware](#) on page 80.

## Dashboard (BASIC Home Screen)

The modem router BASIC Home screen has a dashboard that lets you see the status of your Internet connection and network at a glance. You can click any of the six sections of the dashboard to view and change the settings. The left column has menus. You can use the ADVANCED tab to access more menus and screens.

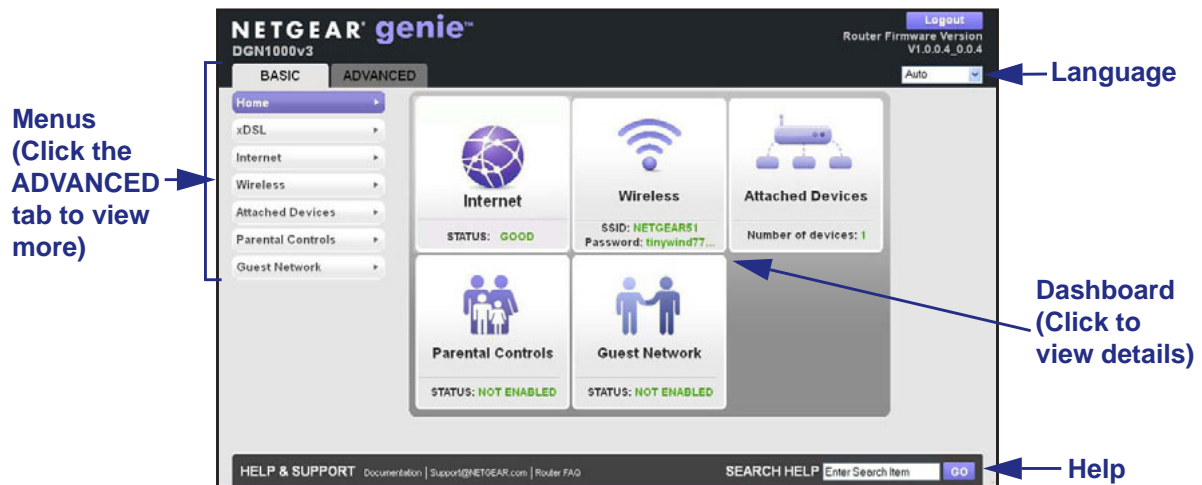


Figure 9. BASIC Home screen with dashboard, language, and online help

- **Home.** This dashboard screen displays when you log in to the modem router.
- **Language.** Select your language from the menu.
- **Internet.** Set, update, and check the ISP settings of your modem router.
- **Wireless.** View or change the wireless settings for your modem router.
- **Attached Devices.** View the devices connected to your network.
- **Parental Controls.** Download and set up parental controls to prevent objectionable content from reaching your computers.
- **Guest Network.** Set up a guest network to allow visitors to use your modem router's Internet connection.
- **ADVANCED tab.** Set the modem router up for unique situations such as when remote access by IP or by domain name from the Internet is needed. See [Chapter 7, Advanced Settings](#). You need a solid understanding of networking to use this tab.
- **Help & Support.** Go to the NETGEAR support site to get information, help, and product documentation. These links work after you have an Internet connection.

## Join Your Wireless Network

You can use the manual or the WPS method to join your wireless network. For instructions about how to set up a guest network, see [Set Up a Guest Network](#) on page 43.

### Manual Method

With the manual method, choose the network that you want and type its password to connect.

➤ **To connect manually:**

1. On your computer or wireless device, open the software that manages your wireless connections.

This software scans for all wireless networks in your area.

2. Look for your network and select it.

The unique WiFi network name (SSID) and password are on the modem router label. If you changed these settings, look for the network name that you used.


3. Enter the modem router password.
4. Click the **Connect** button.

### Wi-Fi Protected Setup Method

Wi-Fi Protected Setup (WPS) lets you connect to a secure WiFi network without typing its password. Instead, press a button or enter a PIN. NETGEAR calls WPS Push 'N' Connect.

Some older WiFi equipment is not compatible with WPS. WPS works only with WPA2 or WPA wireless security.

➤ **To use WPS to join the wireless network:**

1. Press the **WPS** button on the modem router front panel .
2. Within two minutes, press the **WPS** button on your wireless device, or follow the WPS instructions that came with the device.

The WPS process automatically sets up your wireless computer with the network password and connects you to the wireless network.

## NETGEAR genie App and Mobile genie App

The genie app is the easy dashboard for managing, monitoring, and repairing your home network. See the *NETGEAR genie App User Manual* for details about the genie apps.

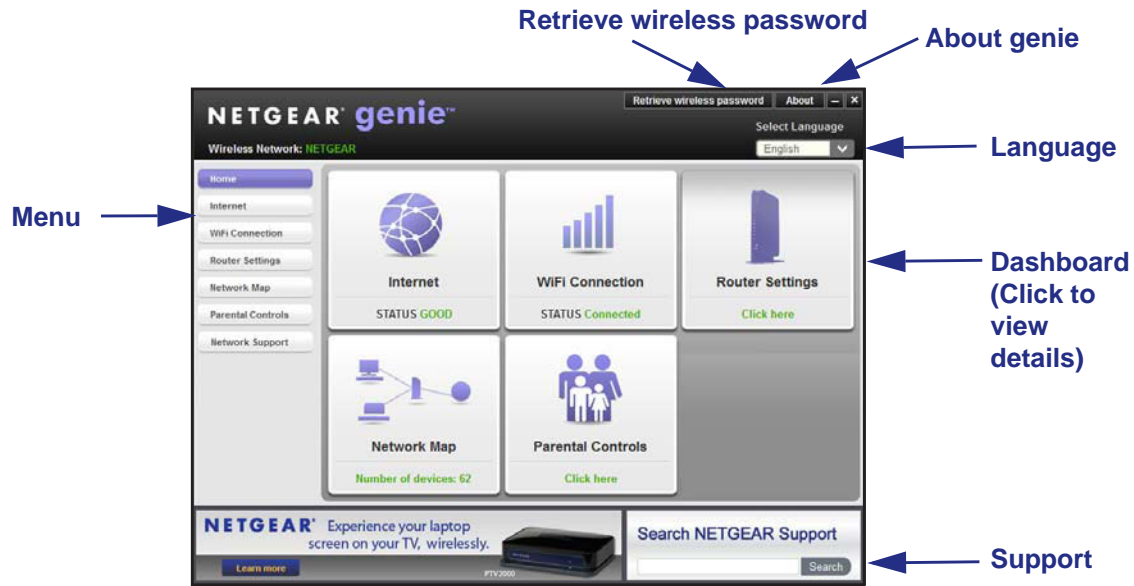


Figure 10. genie app dashboard

The genie app can help you with the following:

- Automatically repair common wireless network problems.
- Have easy access to features like Live Parental Controls, guest access, Internet traffic meter, speed test, and more.

The genie mobile app works on your iPhone, iPad, or Android phone:

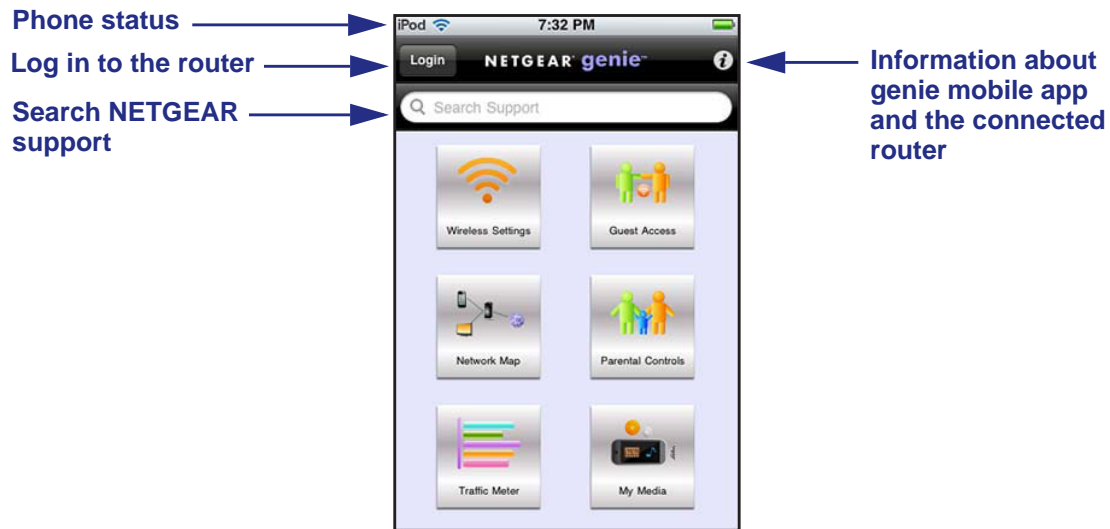


Figure 11. genie mobile app home screen

# 3. NETGEAR genie Basic Settings

---

# 3

Your Internet connection and WiFi network

This chapter contains the following sections:

- *Internet Setup*
- *xDSL Setup*
- *Parental Controls*
- *Basic Wireless Settings*
- *Set Up a Guest Network*
- *View Attached Devices*

## Internet Setup

NETGEAR recommends that you use the Setup Wizard to detect the Internet connection and automatically set up the modem router (see *Internet Connection Setup Wizard* on page 47).

You can view or change the basic ISP information on the Internet Setup screen.

If your ISP provides you with regular Internet service and Internet protocol television (IPTV) service, you must configure the Internet settings for both interface WAN1 and interface WAN2, as directed by your ISP. In that case, complete the following procedure twice, once for interface WAN1 and once for interface WAN2, using the information that your IPS provides to you.

➤ **To view or change the basic Internet setup:**

1. From the Home screen, select **Internet**.

**Internet Setup**

Test Cancel Apply

WAN 1 Router Mode

Does your Internet connection require a login?

Yes  
 No

Encapsulation: PPPoE(PPP over Ethernet)

T-Online  
 1&1  
 Other

Connection identifier:

T-Online number:

Co-user suffix:

Password:

Service Name (If Required):

Connection Mode: Always On

Idle Timeout (In Minutes):

Internet IP Address

Get Dynamically from ISP  
 Use Static IP Address

IP Address:

Domain Name Server (DNS) Address

Get Automatically from ISP  
 Use These DNS Servers

Primary DNS:

Secondary DNS:

Router MAC Address

Use Default Address  
 Use Computer MAC Address  
 Use This MAC Address:

NAT (Network Address Translation):  Enable  Disable



The fields that display on the Internet Setup screen depend on whether your Internet connection requires a login.

If your Internet connection does require a login, the fields that display also depend on the selected encapsulation method and whether you select the T-Online, T&T, or Other radio button. The settings are described in the following sections.

2. From WAN menu in the upper left of the screen, select the WAN interface, as directed by your ISP.
  - **WAN1.** Interface WAN2 is used for regular Internet service. This is the default selection.
  - **WAN2.** Interface WAN2 is used for IPTV only. When you select **WAN2**, the No radio button is selected automatically, and the screen adjusts.

**Note:** *The Router Mode menu next to the WAN menu is fixed at the Router Mode selection.*

3. If you selected WAN1 from the WAN menu, select the **Yes** or **No** radio button.
  - **Yes.** Select the encapsulation method and enter the login name. If you want to change the login time-out, enter a new value in minutes.
  - **No.** Enter the account and domain names, only if needed.

4. Enter the settings for the IP address and DNS server.

The default settings usually work fine. If you have problems with your connection, check the ISP settings.

5. Click the **Apply** button.

Your settings are saved.

6. To test your Internet connection, click the **Test** button.

If the NETGEAR website does not display within one minute, see [Chapter 8, Troubleshooting](#).

The following sections describe all of the possible fields on the Internet Setup screen.

## Internet Setup Screen Fields: No Login Required

These fields display only when no login is required, that is, when you select **No** radio button.

- **Account Name (If required).** Enter the account name provided by your ISP. This might also be called the host name.
- **Domain Name (If required).** Enter the domain name provided by your ISP.

### Internet IP Address.

- **Get Dynamically from ISP.** Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses.

- **Use Static IP Address.** Enter the IP address, IP subnet mask, and the gateway IP address that your ISP assigned. The gateway is the ISP's modem router to which your modem router connects.
- **Use IP Over ATM (IPoA).** Enter the IP address, IP subnet mask, and the gateway IP address that your ISP assigned for your IPoA service. The gateway is the ISP's modem router to which your modem router connects.

For the Domain Name Server (DNS) Address, Router MAC Address, and NAT (Network Address Translation) sections, see *Internet Setup Screen Fields: Fields That Display Irrespective of Whether Login Is Required* on page 30.

## Internet Setup Screen Fields: Login Required

These fields display only when your ISP requires a login, that is, when you select the **Yes** radio button. The fields that display also depend on the selected encapsulation method and whether you select the T-Online, T&T, or Other radio button.

### *Encapsulation is PPPoE and Your ISP is T-Online*

These fields display only when you select **PPPoE** from the Encapsulation menu and the **T-Online** radio button.

The screenshot shows the 'Internet Setup' screen with the following fields and options:

- Encapsulation:** A dropdown menu set to 'PPPoE(PPP over Ethernet)'.
- Radio Buttons:** 'T-Online' is selected (indicated by a filled circle), with '1&1' and 'Other' unselected.
- Connection identifier:** An empty text input field.
- T-Online number:** A text input field containing the number '0'.
- Co-user suffix:** An empty text input field.
- Password:** An empty text input field.
- Service Name (If Required):** An empty text input field.
- Connection Mode:** A dropdown menu set to 'Always On'.
- Idle Timeout (In Minutes):** A text input field containing the number '5'.

Figure 12. Internet Setup screen: fields that are specific to the T-Online selection

- **Connection identifier.** The connection identifier that T-Online provides.
- **T-Online number.** The online number that T-Online provides.
- **Co-user suffix.** The co-user suffix that T-Online provides.
- **Password.** The password that you use to log in to T-Online.
- **Service Name (if Required).** If T-Online provided a service name, enter it here.
- **Connection Mode.** This field is masked out and not available.
- **Idle Timeout (In Minutes).** This field is masked out and not available.

### Internet IP Address.

- **Get Dynamically from ISP.** T-Online uses DHCP to assign your IP address. T-Online automatically assigns these addresses.
- **Use Static IP Address.** Enter the static IP address that T-Online provides.

For the Domain Name Server (DNS) Address, Router MAC Address, and NAT (Network Address Translation) sections, see *Internet Setup Screen Fields: Fields That Display Irrespective of Whether Login Is Required* on page 30.

### Encapsulation is PPPoE and Your ISP is 1&1

These fields display only when you select **PPPoE** from the Encapsulation menu and the **1&1** radio button.

The screenshot shows the 'Encapsulation' section of the Internet Setup screen. The 'Encapsulation' dropdown menu is set to 'PPPoE(PPP over Ethernet)'. Below this, there are three radio buttons: 'T-Online', '1&1' (which is selected), and 'Other'. The 'Login' field is pre-filled with '1und1/' and has a text input field followed by '@online.de'. The 'Password' field is a text input field. The 'Service Name (If Required)' field is a text input field. The 'Connection Mode' dropdown menu is set to 'Always On'. The 'Idle Timeout (In Minutes)' field is a text input field with the value '5'.

Figure 13. Internet Setup screen: fields that are specific to the 1&1 selection

- **Login.** The login name that you use to log in to 1&1. The name has a prefix of 1und1/ and an affix of @online.de. For example, if your login name is ABCDE, the entire login string automatically becomes 1und1/ABCDE@online.de.
- **Password.** The password that you use to log in to 1&1.
- **Service Name (if Required).** If 1&1 provided a service name, enter it here.
- **Connection Mode.** This field is masked out and not available.
- **Idle Timeout (In Minutes).** This field is masked out and not available.

### Internet IP Address.

- **Get Dynamically from ISP.** 1&1 uses DHCP to assign your IP address. 1&1 automatically assigns these addresses.
- **Use Static IP Address.** Enter the static IP address that 1&1 provides.

For the Domain Name Server (DNS) Address, Router MAC Address, and NAT (Network Address Translation) sections, see *Internet Setup Screen Fields: Fields That Display Irrespective of Whether Login Is Required* on page 30.

## Encapsulation is PPPoE and Your ISP is Other

These fields display only when you select **PPPoE** from the Encapsulation menu and the **Other** radio button.

The screenshot shows the 'Internet Setup' screen with the 'Encapsulation' dropdown set to 'PPPoE (PPP over Ethernet)'. Underneath, three radio buttons are visible: 'T-Online', '1&1', and 'Other', with 'Other' selected. Below the radio buttons are several input fields: 'Login' (containing 'guest'), 'Password' (empty), 'Service Name (If Required)' (empty), 'Connection Mode' (a dropdown menu showing 'Always On'), and 'Idle Timeout (In Minutes)' (containing '5').

Figure 14. Internet Setup screen: fields that are specific to the Other selection

- **Login.** The login name that you use to log in to your ISP. By default, the login name is guest.
- **Password.** The password that you use to log in to your ISP.
- **Service Name (if Required).** If your ISP provided a service name, enter it here.
- **Connection Mode.** This field is masked out and not available.
- **Idle Timeout (In Minutes).** This field is masked out and not available.

### Internet IP Address.

- **Get Dynamically from ISP.** Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses.
- **Use Static IP Address.** Enter the static IP address that your ISP provides.

For the Domain Name Server (DNS) Address, Router MAC Address, and NAT (Network Address Translation) sections, see *Internet Setup Screen Fields: Fields That Display Irrespective of Whether Login Is Required* on page 30.

## Encapsulation is PPPoA

These fields display only when you select **PPPoA** from the Encapsulation menu. You cannot select an ISP radio button with the PPPoA selection.

Encapsulation	PPPoA(PPP over ATM) ▼
Login	guest
Password	<input type="text"/>
Service Name (If Required)	<input type="text"/>
Connection Mode	Always On ▼
Idle Timeout (In Minutes)	5

Figure 15. Internet Setup screen: fields that are specific to PPPoA encapsulation

- **Login.** The login name that you use to log in to your ISP. By default, the login name is guest.
- **Password.** The password that you use to log in to your ISP.
- **Service Name (if Required).** If your ISP provided a service name, enter it here.
- **Connection Mode.** This field is masked out and not available.
- **Idle Timeout (In Minutes).** In almost most scenarios, this field is masked out and is not available. If it is available and you want to change the login time-out, enter a new value in minutes. This setting determines how long the modem router keeps the Internet connection active after there is no Internet activity from the LAN. A value of 0 (zero) means never log out. The default setting is 5 seconds.

### Internet IP Address.

- **Get Dynamically from ISP.** Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses.
- **Use Static IP Address.** Enter the static IP address that your ISP provides.

For the Domain Name Server (DNS) Address and NAT (Network Address Translation) sections, see the following section, *Internet Setup Screen Fields: Fields That Display Irrespective of Whether Login Is Required*.

## Internet Setup Screen Fields: Fields That Display Irrespective of Whether Login Is Required

These fields display irrespective of whether your ISP requires a login:

**Domain Name Server (DNS) Address.** The DNS server is used to look up site addresses based on their names.

- **Get Automatically from ISP.** Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address.
- **Use These DNS Servers.** If you know that your ISP requires specific servers, select this option. Enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.

**Router MAC Address.** The Ethernet MAC address that the modem router uses on the Internet port. Some ISPs register the MAC address of the network interface card in your computer when your account is first opened. They accept traffic only from the MAC address of that computer. This feature allows your modem router to use your computer's MAC address (also called cloning).

- **Use Default Address.** Use the default MAC address.
- **Use Computer MAC Address.** The modem router captures and uses the MAC address of the computer that you are now using. You must use the one computer that the ISP allows.
- **Use This MAC Address.** Enter the MAC address that you want to use.

**NAT (Network Address Translation).** NAT allows computers on your home network to share the modem router Internet connection. NAT is enabled by default because it is needed in most situations. The following settings are available:

- **Enable.** NAT is enabled. This is the default setting.
- **Disable.** NAT is disabled.

## xDSL Setup

NETGEAR recommends that you use the Setup Wizard to detect the DSL connection and automatically set up the modem router (see *Internet Connection Setup Wizard* on page 47).

If you have technical experience and are sure of the correct DSL mode, multiplexing method, and virtual circuit number for the virtual path identifier (VPI) and virtual channel identifier (VCI), you can specify those settings on the xDSL Setup screen. NETGEAR recommends that you change the WAN interface selection and enter the multiplexing method, VPI, VCI, and VLAN ID only if your ISP provided you this information.

Use interface WAN1 for regular Internet service. Use interface WAN2 for Internet protocol television (IPTV) service. If your ISP provides IPTV service in addition to regular Internet service, you must configure both interface WAN1 and interface WAN2. If your ISP does not provide IPTV service to you, do not configure and enable interface WAN2.

## Configure Regular Internet Service

The modem router uses interface WAN1 for regular Internet service.

➤ **To configure the DLS setup for regular Internet service:**

**1. Select BASIC > xDSL Setup.**

The screenshot shows the 'xDSL Setup' configuration page. It includes the following fields and options:

- Physical WAN Type:** ADSL2+ (dropdown menu)
- DSL Mode:** Auto (dropdown menu)
- Apply** (green button)
- WAN 1** (dropdown menu)
- PVC Settings:**
  - Enable This Interface
  - Multiplexing Method:** LLC-BASED (dropdown menu)
  - VPI:** 1 (text input)
  - VCI:** 32 (text input)
  - Use VLANID
  - VLANID:** 7 (text input)
- Apply** (green button)

The selection from the Physical WAN Type menu is fixed at ADSL2+.

2. From the DSL Mode menu, select the DSL mode that your ISP provided you:
  - **Auto.** The modem router detects the DSL mode automatically. This is the default setting.
  - **ADSL (g.dmt).**
  - **ADSL2.**
  - **ADSL2+.**
3. Click the upper **Apply** button.  
The DSL mode is saved.
4. From the WAN menu, select **WAN1**.  
WAN 1 is used for normal Internet service. This is the default selection.
5. Leave the **Enable This Interface** check box selected.  
This is the default selection for interface WAN1.
6. From the Multiplexing Method menu, select **LLC-based** or **VC-based**, as indicated by your ISP.
7. For the VPI, type a number between 0 and 255, as indicated by your ISP.  
The default setting is 0.
8. For the VCI, type a number between 32 and 65535, as indicated by your ISP.

The default setting is 38.

9. Depending on your configuration, either disable or configure and enable the VLAN:
  - If you do *not* use interface WAN2 for IPTV service, clear the **Use VLANID** check box.  
The check box might be cleared by default.
  - If you do use interface WAN2 for IPTV service (see the next section, *Configure IPTV Service*), configure the following settings:
    - Enter the VLAN ID, as indicated by your ISP.  
If you select T-Online as your service provider (see *Internet Setup* on page 24), the default VLAN ID is 7.
    - Select the **Use VLANID** check box.  
If you select T-Online as your service provider (see *Internet Setup* on page 24), this check box is selected by default.
10. Click the lower **Apply** button.  
The WAN1 interface and PVC settings are saved.
11. If you do *not* use interface WAN2 for IPTV service, make sure that interface WAN2 is disabled:
  - a. From the WAN menu, select **WAN2**.
  - b. Clear the **Enable This Interface** check box.
  - c. Click the lower **Apply** button.  
Interface WAN2 is disabled.

## Configure IPTV Service

The modem router uses interface WAN2 only for Internet protocol television (IPTV) service.

- **To configure the DLS setup for IPTV service:**
  1. Select **BASIC > xDSL Setup**.  
The xDSL screen displays (see the figure on the next page).  
The selection from the Physical WAN Type menu is fixed at ADSL2+.
  2. From the DSL Mode menu, select the DSL mode that your ISP provided you:
    - **Auto**. The modem router detects the DSL mode automatically. This is the default setting.
    - **ADSL (g.dmt)**.
    - **ADSL2**.
    - **ADSL2+**.
  3. Click the upper **Apply** button.  
The DSL mode is saved.



**xDSL Setup**

Physical WAN Type: ADSL2+

DSL Mode: Auto

**Apply**

WAN 2

**PVC Settings**

Enable This Interface

Multiplexing Method: LLC-BASED

VPI: 1

VCI: 32

Use VLANID

8

**Apply**

- From the WAN menu, select **WAN2**.

Interface WAN2 is used for IPTV only. The screen adjusts. The Multiplexing Method menu becomes unavailable and the default VLAN ID changes to 8, but the Use VLANID check box remains cleared.

- Select the **Enable This Interface** check box.

If you select T-Online as your service provider (see [Internet Setup](#) on page 24), this check box is selected by default for interface WAN2. For other service providers, this check box might be cleared for interface WAN2.

**Note:** *The Multiplexing Method menu is disabled for interface WAN2.*

- For the VPI, type a number between 0 and 255, as indicated by your ISP.  
The default setting is 0.
- For the VCI, type a number between 32 and 65535, as indicated by your ISP.  
The default setting is 38.
- Enter the VLAN ID, as indicated by your ISP.

If you select T-Online as your service provider (see [Internet Setup](#) on page 24), the default VLAN ID is 8.

- Select the **Use VLANID** check box.

If you select T-Online as your service provider (see [Internet Setup](#) on page 24), this check box is selected by default for interface WAN2.

- Click the lower **Apply** button.

The WAN2 interface and PVC settings are saved.

## Parental Controls

The first time you select Parental Controls from the BASIC Home screen, your browser goes to the Live Parental Controls website. You can learn more about Live Parental Controls or download the application.



Figure 16. Live Parental Controls website

➤ **To set up Live Parental Controls:**

1. Select **Parental Controls** on the dashboard screen.
2. Click either the **Windows Users** or **Mac Users** button.
3. Follow the onscreen instructions to download and install the NETGEAR Live Parental Controls Management utility.

After installation, Live Parental Controls automatically starts.



- 4. Click the **Next** button, read the note, and click the **Next** button again to proceed.

Because Live Parental Controls uses free OpenDNS accounts, you are prompted to log in or create a free account.

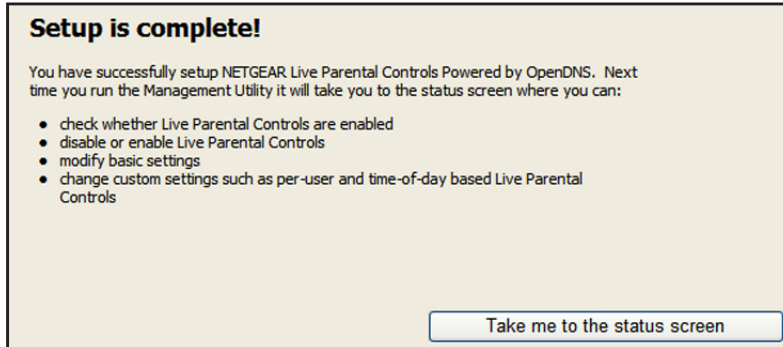
- 5. Select the radio button that applies to you and click the **Next** button.
  - If you already have an OpenDNS account, leave the **Yes** radio button selected.
  - If you do not have an OpenDNS account, select the **No** radio button.

If you are creating an account, the following screen displays:

- a. Fill in the fields.
- b. Click the **Next** button.

After you log on or create your account, the filtering level screen displays:

6. Select the radio button for the filtering level that you want and click the **Next** button.



7. Click the **Take me to the status screen** button.

Parental controls are now set up for the modem router. The dashboard shows Parental Controls as Enabled.

## Basic Wireless Settings

The Wireless Settings screen lets you view or configure the wireless network setup.

The modem router comes with preset security. This means that the WiFi network name (SSID), network key (password), and security option (encryption protocol) are preset in the factory. You can find the preset SSID and password on the label of the unit.

---

**Note:** The preset SSID and password are uniquely generated for every device to protect and maximize your wireless security.

---

*NETGEAR recommends that you do not change your preset security settings.* If you change your preset security settings, make a note of the new settings and store it in a safe place where you can easily find it.

If you use a wireless computer to change the wireless network name (SSID) or other wireless security settings, you are disconnected when you click the Apply button. To avoid this problem, use a computer with a wired connection to access the modem router.

➤ **To view or change basic wireless settings:**

1. Select **BASIC > Wireless**.

The screen sections, settings, and procedures are explained in the following sections.

2. Change the settings as needed.
3. Click the **Apply** button.

Your settings are saved.

If you were connected wirelessly to the modem router and you changed the SSID or wireless security, you are disconnected from the network.

4. If you changed the settings, make sure that you can connect wirelessly to the network with its new settings.

If you cannot connect wirelessly, check the following:

- Is your computer or wireless device connected to another wireless network in your area? Some wireless devices automatically connect to the first open network (without wireless security) that they discover.
- Is your computer or wireless device trying to connect to your network with its old settings (before you changed the settings)? If so, update the wireless network selection in your computer or wireless device to match the current settings for your network.

## Wireless Settings Screen Fields

You can use this screen to view or change the wireless network settings and the security option.

- **Enable SSID Broadcast.** This feature allows the modem router to broadcast its SSID so wireless stations can see this wireless name (SSID) in their scanned network lists. This check box is selected by default. To turn off the SSID broadcast, clear this check box, and click the **Apply** button.
- **Enable Wireless Isolation.** If this check box is selected, computers or wireless devices that join the network can use the Internet, but cannot access each other or access Ethernet devices on the network.
- **Name (SSID).** The SSID is also known as the wireless network name. Enter a 32-character (maximum) name in this field. This field is case-sensitive. The default SSID is randomly generated, and *NETGEAR strongly recommends that you do not change this setting.*
- **Region.** The location where the modem router is used. Select from the countries in the menu. In the United States, the region is fixed to North America and is not changeable.
- **Channel.** This setting is the wireless channel the modem router uses. The default setting is Auto, which allows the modem router to select the channel automatically. You can also enter a value from 1 through 13. (For products on the North American market, only Channels 1 through 11 can be operated.) Do not change the channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, experiment with different channels to see which is the best.

To reduce interference when you use multiple access points, ensure that adjacent access points use different radio frequency channels. The recommended channel spacing between adjacent access points is four channels (for example, use Channels 1 and 5, or 6 and 10).

- **Mode.** Up to 65 Mbps is the default setting. The other settings are Up to 54 Mbps, and Up to 150 Mbps:
  - Up to 54 Mbps allows 802.11g and 802.11b devices to join the network. This is a legacy mode that does not support 802.11n devices in the network.
  - Up to 65 Mbps allows 802.11n, 802.11g, and 802.11b devices to join the network. This mode works well for most networks.
  - Up to 150 Mbps allows 802.11n, 802.11g, and 802.11b devices to join the network. Use this mode if most devices in the network support 802.11n.
- **Security Options.** The modem router comes with unique preset wireless security. These settings are on the product label. NETGEAR recommends that you use preset security so that you can refer to the label if you forget the WiFi password. However, you can change the security option and passphrase. If you want to change the security options, see the following sections.

## Security Options: WPA-PSK, WPA2-PSK, and WPA-PSK + WPA2-PSK Mixed Mode

WPA encryption is built into all hardware that has the Wi-Fi-certified seal. This seal means that the product is authorized by the Wi-Fi Alliance (<http://www.wi-fi.org/>) because it complies with the worldwide single standard for high-speed wireless local area networking.

These types of wireless security options use a pre-shared key (PSK), which is the same as a passphrase, wireless network password, or network key. For help with WPA settings on your wireless computer or device, see the instructions that came with your product.

You can select from the following wireless PSK security options:

- **WPA-PSK [TKIP]**. Wi-Fi Protected Access (WPA) provides strong data security with Temporal Key Integrity Protocol (TKIP) encryption. This option supports speeds of up to 54 Mbps only.
- **WPA2-PSK [AES]**. Wi-Fi Protected Access version 2 (WPA2) provides strong data security with Advanced Encryption Standard (AES) encryption. This is the preset wireless security that is enabled by default. WPA2 provides the most reliable security. This option supports speeds of up to 150 Mbps. If not all clients in your network support WPA2, select WPA-PSK + WPA2-PSK mixed mode.
- **WPA-PSK [TKIP] + WPA2-PSK [AES]**. WPA-PSK + WPA2-PSK is referred to as mixed mode, which supports a combination of TKIP and AES encryption for both WPA and WPA2 clients. For WPA clients, this option supports speeds of up to 54 Mbps only. For WPA2 clients, this option supports speeds of up to 150 Mbps.

### ➤ To change the WPA wireless security option and passphrase:

1. Select **BASIC > Wireless**.

The Wireless Settings screen displays.

2. In the Security Options section, select one of the WPA options with PSK:

- **WPA-PSK [TKIP]**
- **WPA2-PSK [AES]**
- **WPA-PSK [TKIP] + WPA2-PSK [AES]**

**Security Options**

None  
 WEP  
 WPA-PSK [TKIP]  
 WPA2-PSK [AES]  
 WPA-PSK [TKIP] + WPA2-PSK [AES]  
 WPA/WPA2 Enterprise

---

**Security Options (WPA2-PSK)**

Passphrase :  (8-63 characters or 64 hex digits)

3. In the associated Passphrase field, enter the passphrase that you want to use.



The passphrase is a text string from 8 to 63 ASCII characters or exactly 64 hexadecimal digits. A hexadecimal digit is one of the following characters: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F (uppercase or lowercase).

Wireless clients must use the passphrase to access the wireless network through the modem router.

4. Click the **Apply** button.

## Security Options: WPA/WPA2 Enterprise

This security option is not for home use but is typically used in a business or enterprise. WPA/WPA2 Enterprise does not use a passphrase but supports 802.1x authentication, which requires an internal or external RADIUS server. A Remote Authentication Dial In User Service (RADIUS) server provides Authentication, Authorization, and Accounting (AAA) management to grant (or deny) computers access to your wireless network.

WPA/WPA2 Enterprise can support WPA [TKIP] for WPA clients only, WPA2 [AES] for WPA2 clients only, and WPA [TKIP] + WPA2 [AES], which is a combination of TKIP and AES encryption, for both WPA and WPA2 clients. WPA clients are supported at speeds of up to 54 Mbps only. WPA2 clients are supported at speeds of up to 300 Mbps.

WPA/WPA2 Enterprise supports five Extensible Authentication Protocol (EAP) authentication methods: EAP-TLS, EAP-TTLS/MSCHAPv2, PEAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, and EAP-SIM.

### ➤ To configure WPA/WPA2 Enterprise security:

1. Select **BASIC > Wireless**.

The Wireless Settings screen displays.

2. In the Security Options section, select the **WPA/WPA2 Enterprise** radio button.

**Security Options**

None  
 WEP  
 WPA-PSK [TKIP]  
 WPA2-PSK [AES]  
 WPA-PSK [TKIP] + WPA2-PSK [AES]  
 WPA/WPA2 Enterprise

---

**Security Options ( WPA/WPA2 Enterprise )**

WPA Mode: WPA [TKIP] + WPA2 [AES] ▼

RADIUS server IP Address: . . .

RADIUS server Port: 1812

RADIUS server Shared Secret:



3. Select the WPA mode:
  - **WPA [TKIP]**
  - **WPA2 [AES]**
  - **WPA [TKIP] + WPA2 [AES]**
4. Type the IP address of the RADIUS server.

The address can be on your LAN or it can be an external address.
5. Enter the port number for the RADIUS server in the range from 1 to 6553.

The default number is 1812.
6. Type the shared secret, which needs to be between 1 and 128 characters.

The default value is blank.

The shared secret is case-sensitive.
7. Click the **Apply** button.

## Security Options: WEP

Wired Equivalent Privacy (WEP) security is a legacy authentication and data encryption mode that has been superseded by WPA-PSK and WPA2-PSK. WEP supports speeds of up to 54 Mbps (the modem router can support speeds of up to 150 Mbps) and does not function with WPS. However, if you set up a wireless distribution system (WDS; see *Wireless Distribution System* on page 103), WEP is the only security that can be supported.

---

**Note:** The WEP option displays only if you select Up to 54 Mbps from the Mode menu.

---

➤ **To configure WEP security:**

1. Select **BASIC > Wireless**.

The Wireless Settings screen displays.
2. In the Security Options section, select the **WEP** radio button.

3. From the Authentication Type menu, select one of the following types:
  - **Shared Key.** Clients can use only shared key authentication.
  - **Automatic.** Client can use either open system or shared key authentication.
4. From the Encryption Strength menu, select the encryption key size:
  - **64-bit.** Standard WEP encryption, using 40/64-bit encryption.
  - **128-bit.** Standard WEP encryption, using 104/128-bit encryption. This selection provides higher encryption security.
5. Generate the key automatically or enter it manually:
  - Automatic key generation:
    - a. In the Passphrase field, enter a passphrase:
    - b. Click the **Generate** button.

For 64-bit WEP, four different WEP keys are generated. For 128-bit WEP, only one WEP key is generated, and the four key fields are populated with the same WEP key.
  - Manual key generation:
    - a. Specify the active key by selecting the **Key 1**, **Key 2**, **Key 3**, or **Key 4** radio button.
 

Only one key can be the active key.
    - b. Enter the value for the key manually:
      - For 64-bit WEP, enter 10 hexadecimal digits (any combination of 0–9, A–F). The key values are not case-sensitive.
      - For 128-bit WEP, enter 26 hexadecimal digits (any combination of 0–9, A–F). The key values are not case-sensitive.
6. Click the **Apply** button.

## Set Up a Guest Network

Adding a guest network allows visitors at your home to use the Internet without using your wireless security key. You can set up to three guest networks, all of which can be active at a same time. However, if all three guest networks are active, only one is displayed on the Router Status screen (see [View Router Status](#) on page 82). By default, none of the guest networks are enabled.

➤ **To set up a guest network:**

1. Select **BASIC > Guest Network**.

**Guest Network Settings**

Cancel Apply

Profile	SSID	Security	Enable	Broadcast SSID
<input checked="" type="radio"/> 1	NETGEAR-Guest1	WPA2-PSK [AES]	No	Yes
<input type="radio"/> 2	NETGEAR-Guest2	None	No	Yes
<input type="radio"/> 3	NETGEAR-Guest3	None	No	Yes

**Wireless Settings - Profile 1**

Enable Guest Network

Enable SSID Broadcast

Allow guest to access My Local Network

Enable Wireless Isolation

Guest Wireless Network Name (SSID):

**Security Options - Profile 1**

None

WEP

WPA-PSK [TKIP]

WPA2-PSK [AES]

WPA-PSK [TKIP] + WPA2-PSK [AES]

WPA/WPA2 Enterprise

**Security Options (WPA2-PSK)**

Passphrase:  (8-63 characters or 64 hex digits)

2. In the Network Profiles table, select the radio button to the left of the profile that you want to set up.
3. Select any of the following wireless settings:
  - **Enable Guest Network.** When this check box is selected, the guest network is enabled, and guests can connect to your network using the SSID of this profile.
  - **Enable SSID Broadcast.** If this check box is selected, the wireless access point broadcasts its name (SSID) to all wireless stations. Stations with no SSID can adopt the correct SSID for connections to this access point.
  - **Allow guest to access My Local Network.** If this check box is selected, anyone who connects to this SSID has access to your local network, not just Internet access.
  - **Enable Wireless Isolation.** If this check box is selected, wireless computers or devices that join the network can use the Internet but cannot access each other or access Ethernet devices on the network.

- (Optional) Change the name of the guest network.

The default names are NETGEAR-Guest1, NETGEAR-Guest2, and NETGEAR-Guest3.

The guest network name is case-sensitive and can be up to 32 characters. You then manually configure the wireless devices in your network to use the guest network name in addition to the main SSID.

- Select a security option from the menu and configure the associated settings.

The security options are described in the following sections:

- Security Options: WPA-PSK, WPA2-PSK, and WPA-PSK + WPA2-PSK Mixed Mode* on page 39
- Security Options: WPA/WPA2 Enterprise* on page 40
- Security Options: WEP* on page 41

- Click the **Apply** button.

Your settings are saved.

## View Attached Devices

You can view all computers and devices that are currently connected to your network.

- **To go to the Attached Devices screen:**

- From the BASIC Home screen, select **Attached Devices**.

The screenshot shows the 'Attached Devices' screen with a table of connected devices. The table is divided into two sections: 'Wired Devices' and 'Wireless Devices (Wireless intruders also show up here)'. Each section has a header row with columns for device identification and network information. A 'Refresh' button is located at the bottom of the screen.

Wired Devices			
#	IP Address	MAC Address	Device Name
1	192.168.0.200	00:1D:09:AC:AA 7E	Vostro1500

Wireless Devices (Wireless intruders also show up here)			
SSID	IP Address	MAC Address	Device Name
NETGEAR51	192.168.0.2	20:D6:07:2C:70 E5	-

Wired devices are connected to the modem router with Ethernet cables. Wireless devices have joined the wireless network. The following information is displayed:

- #** (number). The order in which the device joined the network.
- IP Address**. The IP address that the modem router assigned to this device when it joined the network. This number can change if a device is disconnected and rejoins the network.

- **MAC Address.** The unique MAC address for each device does not change. The MAC address is typically shown on the product label.
  - **Device Name.** If the device name is known, it is shown here.
2. (Optional) Click the **Refresh** button.  
The information onscreen is updated.

# 4 NETGEAR genie ADVANCED Home

---

# 4

## Specify custom settings

This chapter contains the following sections:

- *NETGEAR genie ADVANCED Home Screen*
- *Internet Connection Setup Wizard*
- *WAN Setup*
- *LAN Setup*
- *WPS Wizard for WiFi Connections*
- *QoS Setup*

The following selections on the ADVANCED Home screen are described in separate chapters:

- **Security.** See *Chapter 5, Security*.
- **Administration.** See *Chapter 6, Administration*.
- **Advanced Setup.** See *Chapter 7, Advanced Settings*.

## NETGEAR genie ADVANCED Home Screen

The genie ADVANCED Home dashboard presents status information. The content is the same as what is on the Router Status screen available from the Administration menu. For more information about the fields on the screen, see [View Router Status](#) on page 82. The genie ADVANCED Home screen is shown in the following figure:

The screenshot displays the NETGEAR genie ADVANCED Home screen. The interface is divided into several sections:

- Navigation:** A sidebar on the left contains buttons for "ADVANCED Home", "Setup Wizard", "WPS Wizard", "Setup", "Security", "Administration", and "Advanced Setup". Under "Setup", there are links for "xDSL Setup", "Internet Setup", "Wireless Setup", "Guest Network", "WAN Setup", "LAN Setup", and "QoS Setup".
- Router Information:** A panel with a green checkmark icon showing:
 

Hardware Version	DGN1000v3-A
Firmware Version	V1.0.0.4_0.0.4AU
GUI Language Version	V1.0.0.7

 Below this is the "LAN Port" section:
 

MAC Address	28:C6:8E:AD:BC:2E
IP Address	192.168.0.1
DHCP Server	On

 A "Reboot" button is located below the LAN Port section.
- Internet Port:** A panel with a green checkmark icon showing:
 

MAC Address	28:C6:8E:AD:BC:2F
IP Address	10.0.0.15
Connection	PPPoE
IP Subnet Mask	255.255.255.255
Domain Name Server	203.0.113.1 203.0.113.2

 "Show Statistics" and "Connection Status" buttons are at the bottom.
- Modem:** A panel with a green checkmark icon showing:
 

xDSL Firmware Version	4925ca26
Modem Status	connected
DownStream Connection Speed	24044
UpStream Connection Speed	1138
VPI	8
VCI	38

 A "Modem Statistics" button is at the bottom.
- Wireless Settings:** A panel with a green checkmark icon showing:
 

Name (SSID)	NETGEAR51
Region	United States
Channel	Auto ( 1 )
Mode	Up to 85 Mbps
Wireless AP	On
Broadcast Name	On
Wireless isolation	Off
Wi-Fi Protected Setup	Configured
- Guest Network:** A panel with a yellow warning icon showing:
 

Name (SSID)	NETGEAR-Guest1
Wireless AP	Off
Broadcast Name	On
Wireless isolation	Off
Allow guest to access My Local Network	Off

## Internet Connection Setup Wizard

You can use the Setup Wizard to detect your DSL and Internet settings and automatically set up your modem router. The Setup Wizard is not the same as the genie screens that display the first time you connect to your modem router to set it up.

➤ **To use the Setup Wizard:**

1. Select **ADVANCED > Setup Wizard**.

2. From the Country menu, select your location.

**Note:** If you have purchased the modem router in the US, you cannot change the country, and the selection is fixed at the US.

3. Select the **Yes** radio button.

If you select No, you are taken to the Internet Setup screen (see [Internet Setup](#) on page 24).

4. Click the **Next** button.

The Setup Wizard searches your Internet connection for servers and protocols to determine your ISP configuration.

click here to enable wireless security and protect your network.' At the bottom, there are two buttons: 'Print this' and 'Take me to the Internet'."/>

## Setup Menu

Select **ADVANCED > Setup** to display the Setup menu. The following selections are available:

- **xDSL Setup.** This is a shortcut to the same xDSL Setup screen that you can access from the dashboard on the BASIC Home screen. For information, see [xDSL Setup](#) on page 30.
- **Internet Setup.** This is a shortcut to the same Internet Setup screen that you can access from the dashboard on the BASIC Home screen. For information, see [Internet Setup](#) on page 24.



- **Wireless Setup.** This is a shortcut to the same Wireless Settings screen that you can access from the dashboard on the BASIC Home screen. For information, see [Basic Wireless Settings](#) on page 36.
- **Guest Network.** This is a shortcut to the same Guest Network screen that you can access from the dashboard on the BASIC Home screen. For information, see [Set Up a Guest Network](#) on page 43.
- **WAN Setup.** Internet (WAN) setup. For information, see [WAN Setup](#) on page 49.
- **LAN Setup.** Local area network (LAN) setup. For information, see [LAN Setup](#) on page 53.
- **QoS Setup.** Quality of Service (QoS) setup. For information, see [QoS Setup](#) on page 59.

## WAN Setup

The WAN Setup screen lets you configure a DMZ (demilitarized zone) server, change the maximum transmit unit (MTU) size, enable the modem router to respond to a ping on the WAN (Internet) port, and configure other settings for your Internet connection.

### ➤ To view or change the WAN settings:

1. Select **ADVANCED > Setup > WAN Setup**.

The screenshot shows the WAN Setup configuration interface. At the top, there are 'Cancel' and 'Apply' buttons. The settings are organized into sections:

- Disable Port Scan and DoS Protection:** A checkbox that is currently unchecked.
- Default DMZ Server:** A checkbox that is unchecked, followed by four input fields for an IP address, with the first three containing '192', '168', and '0'.
- Respond to Ping on Internet Port:** A checkbox that is unchecked.
- Disable IGMP Proxying:** A checkbox that is checked.
- MTU Size (in bytes):** An input field containing the value '1492'.
- NAT Filtering:** Two radio buttons, 'Secured' (selected) and 'Open'.
- Disable SIP ALG:** A checkbox that is unchecked.
- VPN Passthrough:** Three rows, each with a radio button for 'Enable' (selected) and 'Disable'.

2. Specify the following settings:
  - **Disable Port Scan and DoS Protection.** DoS protection protects your LAN against denial of service attacks such as Syn flood, Smurf Attack, Ping of Death, Teardrop Attack, UDP Flood, ARP Attack, Spoofing ICMP, Null Scan, and many others. Disable this feature only in special circumstances.

- **Default DMZ Server.** This feature is sometimes helpful when you are playing online games or videoconferencing. Be careful when using this feature because it makes the firewall security less effective. For more information, see the following section, [Default DMZ Server](#).
  - **Respond to Ping on Internet Port.** If you want the modem router to respond to a ping from the Internet, select this check box. Use this feature only as a diagnostic tool because it allows your modem router to be discovered. Do not select this check box unless you have a specific reason.
  - **Disable IGMP Proxying.** IGMP proxying allows computers on the LAN to receive the multicast traffic they are subscribed to from the Internet. By default, this check box is selected, and the IGMP proxy is disabled, preventing multicast traffic from the Internet to the LAN. Clear the **Disable IGMP Proxying** check box to allow multicast traffic from the Internet to the LAN.
  - **MTU Size (in bytes).** The normal MTU (maximum transmit unit) value for most Ethernet networks is 1500 bytes, or 1492 bytes for PPPoE connections. For some ISPs, you might need to reduce the MTU. Reduce the MTU only if you are sure that it is necessary for your ISP connection. For more information, see [Change the MTU Size](#) on page 51.
  - **NAT Filtering.** Network Address Translation (NAT) determines how the modem router processes inbound traffic:
    - **Secured NAT.** Provides a secured firewall to protect the computers on the LAN from attacks from the Internet, but might prevent some Internet games, point-to-point applications, or multimedia applications from functioning. By default, the Secured radio button is selected.
    - **Open NAT.** Provides a much less secured firewall, but allows almost all Internet applications to function.
  - **Disable SIP ALG.** The Session Initiation Protocol (SIP) Application Level Gateway (ALG) is enabled by default to optimize VoIP phone calls that use the SIP. Select the **Disable SIP ALG** check box to disable the SIP ALG. Disabling the SIP ALG might be useful when you are running certain applications.
  - **VPN Passthrough.** When the modem router has Network Address Translation (NAT) enabled, it filters encrypted tunnel packets through NAT, causing these packets to become invalid. VPN pass-through allows encrypted tunnel packets to go through without being filtered, and is enabled by default for IPSec, PPTP, and L2TP packets. Do not disable VPN pass-through for IPSec, PPTP, or L2TP unless you have a specific reason.
3. Click the **Apply** button.
- Your settings are saved.

## Default DMZ Server

The default DMZ server feature is helpful when you are using some online games and videoconferencing applications that are incompatible with Network Address Translation (NAT). The modem router is programmed to recognize some of these applications and to work correctly with them, but other applications might not function well. In some cases, one local computer can run the application correctly if the IP address for that computer is entered as the default DMZ server.



### **WARNING:**

**DMZ servers pose a security risk. A computer designated as the default DMZ server loses much of the protection of the firewall and is exposed to exploits from the Internet. If compromised, the DMZ server computer can be used to attack other computers on your network.**

The modem router discards incoming traffic from the Internet that is not a response to one of your local computers or a service that you have set up on the Port Forwarding / Port Triggering screen. Instead of discarding this traffic, you can have the modem router forward the traffic to one computer on your network. This computer is called the default DMZ server.

#### ➤ **To set up a default DMZ server:**

1. Select **ADVANCED > Setup > WAN Setup**.

The WAN Setup screen displays.

2. Select the **Default DMZ Server** check box.
3. Type the IP address.
4. Click the **Apply** button.

Your settings are saved.

## Change the MTU Size

The maximum transmission unit (MTU) is the largest data packet a network device transmits. When one network device communicates across the Internet with another, the data packets travel through many devices along the way. If a device in the data path has a lower MTU setting than the other devices, the data packets are split or “fragmented” to accommodate the device with the smallest MTU.

The best MTU setting for NETGEAR equipment is often just the default value. In some situations, changing the value fixes one problem but causes another. Leave the MTU unchanged unless one of these situations occurs:

- You have problems connecting to your ISP or other Internet service, and the technical support of either the ISP or NETGEAR recommends changing the MTU setting.

These web-based applications might require an MTU change:

- A secure website that does not open, or displays only part of a web page
- Yahoo email
- MSN portal
- America Online's DSL service
- You use VPN and have severe performance problems.
- You used a program to optimize MTU for performance reasons, and now you have connectivity or performance problems.

---

**Note:** An incorrect MTU setting can cause Internet communication problems. For example, you might not be able to access certain websites, frames within websites, secure login pages, or FTP or POP servers.

---

If you suspect an MTU problem, a common solution is to change the MTU to 1400. If you are willing to experiment, you can gradually reduce the MTU from the maximum value of 1500 until the problem goes away. The following table describes common MTU sizes and applications.

**Table 2. Common MTU sizes**

MTU	Application
1500	The largest Ethernet packet size. This setting is typical for connections that do not use PPPoE or VPN, and is the default value for NETGEAR modem routers, adapters, and switches.
1492	Used in PPPoE environments.
1472	Maximum size to use for pinging. (Larger packets are fragmented.)
1468	Used in some DHCP environments.
1460	Usable by AOL if you do not have large email attachments, for example.
1436	Used in PPTP environments or with VPN.
1400	Maximum size for AOL DSL.
576	Typical value to connect to dial-up ISPs.

➤ **To change the MTU size:**

1. Select **ADVANCED > Setup > WAN Setup**.

The WAN Setup screen displays.

2. In the MTU Size field, enter a value from 64 to 1500.
3. Click the **Apply** button.

Your settings are saved.

## LAN Setup

The LAN Setup screen allows configuration of LAN IP services such as Dynamic Host Configuration Protocol (DHCP) and Routing Information Protocol (RIP).

The modem router is shipped preconfigured to use private IP addresses on the LAN side and to act as a DHCP server. The modem router's default LAN IP configuration is:

- **LAN IP address.** 192.168.0.1
- **Subnet mask.** 255.255.255.0

These addresses are part of the designated private address range for use in private networks and are suitable for most applications. If your network requires a different IP addressing scheme, you can change these settings on the LAN Setup screen.

---

**Note:** If you change the LAN IP address of the modem router while connected through the browser, you are disconnected. If you want to continue to use the modem router menus, open a new connection to the new IP address and log in again.

---

### ➤ To change the LAN settings:

1. Select **ADVANCED > Setup > LAN Setup**.

The screenshot shows the LAN Setup configuration interface. At the top, there are 'Cancel' and 'Apply' buttons. The 'Device Name' field is set to 'DGN1000v3'. Under 'LAN TCP/IP Setup', the IP Address is '192.168.0.1' and the Subnet Mask is '255.255.255.0'. The RIP Direction is set to 'Both' and the RIP Version is 'Disabled'. The 'Use Router as DHCP Server' checkbox is checked. The Starting IP Address is '192.168.0.2' and the Ending IP Address is '192.168.0.254'. At the bottom, there is an 'Address Reservation' table with columns for '#', 'IP Address', 'Device Name', and 'MAC Address', and buttons for '+ Add', 'Edit', and 'Delete'.

2. Specify the settings that you want to customize.

These settings are described in the following sections.

3. Click the **Apply** button.

Your settings are saved.

## LAN Setup Screen Settings

The following settings are available.

### *Device Name*

By default, the device name is DGN1000Bv3, which is the modem router model. You can change the device name to another name.

### *LAN TCP/IP Setup*

- **IP Address.** The LAN IP address of the modem router. By default the LAN IP address is 192.168.0.1.
- **IP Subnet Mask.** The LAN subnet mask of the modem router. By default the IP subnet mask is 255.255.255.0. Combined with the IP address, the IP subnet mask allows a device to know which other addresses are local to it, and which addresses must be reached through a gateway or router.
- **RIP Direction.** Router Information Protocol (RIP) allows the modem router to exchange routing information with other routers. This setting controls how the modem router sends and receives RIP packets. Both is the default setting. With the Both or Out Only setting, the modem router broadcasts its routing table periodically. With the Both or In Only setting, the modem router incorporates the RIP information that it receives.
- **RIP Version.** This setting controls the format and the broadcasting method of the RIP packets that the modem router sends. It recognizes both formats when receiving. By default, the RIP function is disabled.
  - **RIP-1** is universally supported. It is adequate for most networks, unless you have an unusual network setup.
  - **RIP-2** carries more information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format. RIP-2B uses subnet broadcasting. RIP-2M uses multicasting.

### *Use Router as DHCP Server*

By default, the Use Router as DHCP Server check box is selected so that the modem router functions as a Dynamic Host Configuration Protocol (DHCP) server.

- **Starting IP Address.** Specify the start of the range for the pool of IP addresses in the same subnet as the modem router. By default, the starting IP address is 192.168.0.2.
- **Ending IP Address.** Specify the end of the range for the pool of IP addresses in the same subnet as the modem router. By default, the ending IP address is 192.168.0.254.

For more information, see *Specify DHCP Server Settings* on page 55.

### *Address Reservation*

When you specify a reserved IP address for a computer on the LAN, that computer receives the same IP address each time it accesses the modem router's DHCP server. Assign reserved IP addresses to servers that require permanent IP settings.

For more information, see [Set Up Address Reservation](#) on page 56.

## Specify DHCP Server Settings

By default, the modem router functions as a DHCP server. The modem router assigns IP, DNS server, and default gateway addresses to all computers connected to the LAN. The assigned default gateway address is the LAN address of the modem router. The modem router assigns IP addresses to the attached computers from a pool of addresses specified on the LAN Setup screen. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN. For most applications, the default DHCP and TCP/IP settings of the modem router work well.

The modem router delivers the following parameters to any LAN device that requests DHCP:

- An IP address from the range that you have defined
- Subnet mask
- Gateway IP address (the modem router's LAN IP address)
- DNS server IP address (the modem router's LAN IP address)

You can specify the pool of IP addresses that the modem router assigns by setting the starting IP address and ending IP address. These addresses must be part of the same IP address subnet as the modem router's LAN IP address. Using the default addressing scheme, define a range between 192.168.1.2 and 192.168.1.254, although you might want to save part of the range for devices with fixed addresses.

### ➤ To specify the pool of IP addresses that the modem router assigns:

#### 1. Select **ADVANCED > LAN Setup**.

The LAN Setup screen displays.

#### 2. Make sure that the **Use Router as a DHCP Server** check box is selected.

#### 3. Specify the range of IP addresses.

For example, using the default addressing scheme, define a range between 192.168.0.2 and 192.168.0.254, although you might want to save part of the range for devices with fixed addresses.

- In the Starting IP Address field, specify the start of the range for the pool of IP addresses in the same subnet as the modem router.
- In the Ending IP Address field, specify the end of the range for the pool of IP addresses in the same subnet as the modem router.

#### 4. Click the **Apply** button.

Your settings are saved.



➤ **To disable the DHCP Server feature on the modem router:**

1. Select **ADVANCED > LAN Setup**.

The LAN Setup screen displays.

2. Clear the **Use Router as DHCP Server** check box.
3. Click the **Apply** button.

Your settings are saved.

4. (Optional) If there is no other DHCP server on your network, set your computers' IP addresses manually so that they can access the modem router.

## Set Up Address Reservation

When you specify a reserved IP address for a computer on the LAN, that computer always receives the same IP address each time it accesses the modem router's DHCP server. NETGEAR recommends that you assign a reserved IP address to a computer or server that requires permanent IP settings.

➤ **To reserve an IP address:**

1. Select **ADVANCED > Setup > LAN Setup**.

The LAN Setup screen displays.

2. In the Address Reservation section of the screen, click the **Add** button.

The screenshot shows the 'Address Reservation' section of the modem router's web interface. At the top, there are three buttons: 'Refresh', 'Cancel', and 'Add'. Below these is a table titled 'Address Reservation Table' with the following data:

#	IP Address	Device Name	MAC Address
1	192.168.0.200	Vostro1500	00:1D:09:AC:AA:7E

Below the table, there are three input fields: 'IP Address' (with a radio button), 'MAC Address', and 'Device Name'.

3. In the IP Address field, type the IP address to assign to the computer or server.

Choose an IP address from the modem router's LAN subnet, such as 192.168.0.x.

**Tip:** If the computer is already on your network, you can select the corresponding radio button from the Address Reservation Table. The computer's information is automatically copied into the IP Address, MAC Address, and Device Name fields.

4. Type the MAC address of the computer or server.
5. (Optional) Type a name for the computer or server.
6. Click the **Apply** button.



The reserved address is entered into the Address Reservation Table on the LAN Setup screen.

The reserved address is not assigned until the next time the computer contacts the modem router's DHCP server. Reboot the computer, or access its IP configuration and force a DHCP release and renew.

➤ **To change a reserved address entry:**

1. Select **ADVANCED > Setup > LAN Setup**.

The LAN Setup screen displays.

2. In the Address Reservation Table, select the radio button next to the reserved address that you want to change.
3. Click the **Edit** button.
4. Change the settings.
5. Click the **Apply** button.

The changes are entered into the Address Reservation Table on the LAN Setup screen.

➤ **To delete a reserved address entry:**

1. Select **ADVANCED > Setup > LAN Setup**.

The LAN Setup screen displays.

2. In the Address Reservation Table, select the radio button next to the reserved address that you want to delete.
3. Click the **Delete** button.

The reserved address is removed from the Address Reservation Table on the LAN Setup screen.

## WPS Wizard for WiFi Connections

The WPS Wizard helps you add a WPS-capable client device (a wireless device or computer) to your network. On the client device, either press its WPS button or locate its WPS PIN.

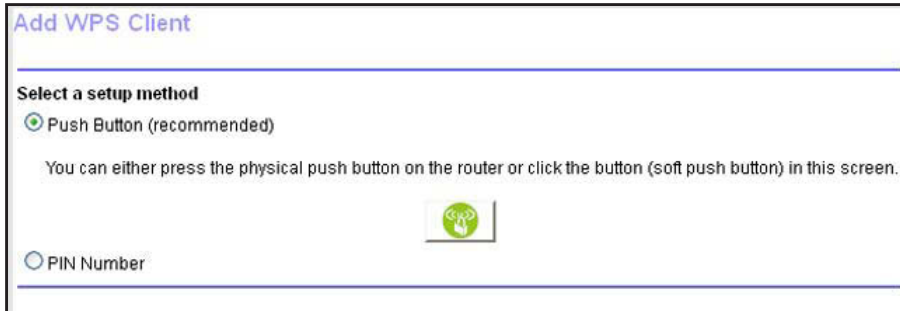
➤ **To use the WPS Wizard:**

1. Select **ADVANCED > WPS Wizard**.

Add WPS Client screen displays.

2. Click the **Next** button.

The following screen lets you select the method for adding the WPS client (a wireless device or computer).




3. Select the radio button for the setup method that you want to use, and follow the steps.

- **Push Button.**
  - a. Either click the **WPS** button on this screen, or press the **WPS** button on the front of the modem router.
  - b. Within two minutes, go to the wireless client and press its **WPS** button to join the network without entering a password.
- **PIN Number.** The screen adjusts.



- a. Enter the client security PIN.
- b. Click the **Next** button.
- c. Within two minutes, go to the client device and use its WPS software to join the network without entering a password.

The modem router attempts to add the WPS-capable device. The WPS LED  on the front of the modem router blinks green. When the modem router establishes a WPS connection, the LED is solid green, and the modem router WPS screen displays a confirmation message.

## QoS Setup

Quality of Service (QoS) is an advanced feature that can be used to prioritize some types of traffic ahead of others. The modem router can provide QoS prioritization over the wireless link and on the Internet connection. You use the QoS Setup screen to set up QoS features.

The following sections describe the QoS features.

### WMM QoS for Wireless Multimedia Applications

The modem router supports Wi-Fi Multimedia Quality of Service (WMM QoS) to prioritize wireless voice and video traffic over the wireless link. WMM QoS, which is enabled by default, provides prioritization of wireless data packets from different applications based on four access categories: voice, video, best effort, and background. For an application to receive the benefits of WMM QoS, both the application and the client running that application must have WMM enabled. Legacy applications that do not support WMM and applications that do not require QoS are assigned to the best effort category, which receives a lower priority than voice and video. WMM QoS is enabled by default.

If the modem router functions in *Up to 65 Mbps* wireless mode or *Up to 150 Mbps* wireless mode, you cannot disable WMM. You can disable WMM only if the modem router functions in *Up to 54 Mbps* wireless mode.

- **To disable WMM QoS if the modem router functions in Up to 54 Mbps wireless mode:**

1. Select **ADVANCED > Setup > QoS Setup**.

The screenshot shows the 'QoS Setup' configuration page. At the top, there are 'Cancel' and 'Apply' buttons. Below are three checked checkboxes: 'Enable WMM (Wi-Fi multimedia) settings', 'Turn Internet Access QoS On', and 'Turn Bandwidth Control On'. Under 'Turn Bandwidth Control On', the 'Uplink bandwidth: Maximum' radio button is selected, and the 'Automatically check Internet Uplink bandwidth: 0 Kbps' radio button is unselected. A 'Check' button is located to the right of the unselected radio button. At the bottom of the page, there is a section titled 'QoS Priority Rule list' with a 'Setup QoS rule' button.

2. Clear the **Enable WMM** check box.
3. Click the **Apply** button.

Your settings are saved.

## Quality of Service Priority Rules and Internet Access

You can give prioritized Internet access to the following types of traffic:

- Specific applications
- Specific online games
- Individual Ethernet LAN ports of the modem router
- A specific device by MAC address

To specify prioritization of traffic, you must create a policy for the type of traffic and add the policy to the QoS Policy table on the QoS Setup screen. (The QoS Policy table displays only after you click the Setup QoS rule button on the QoS Setup screen.) For convenience, the QoS Policy table lists many common applications and online games that can benefit from QoS handling.

By default, QoS is disabled for Internet traffic, the default QoS rules and any custom QoS rules that you created are not activated, and no traffic is prioritized.

### ➤ To enable QoS for Internet traffic and activate the QoS rules:

1. Select **ADVANCED > Setup > QoS Setup**.

2. Select the **Turn Internet Access QoS On** check box.
3. Click the **Apply** button.

Your settings are saved.

The following sections describe how to manage and create QoS rules, which are also referred to as QoS policies.

### Manage QoS Rules

The following procedure refers to preconfigured QoS rules. For information about how to create custom QoS rules, see the sections following this section.

### ➤ To view or change a QoS rule:

1. Select **ADVANCED > Setup > QoS Setup**.

The QoS Setup screen displays.

- Click the **Setup QoS rule** button.

All preconfigured QoS rules are displayed in a table, along with their priority (Highest, High, Normal, or Low) and a description:

#	QoS Policy	Priority	Description
<input type="radio"/> 1	IP Phone (port 6670, includes SIP & H.323 IP phones)	Highest	IP Phone (port 6670, includes SIP & H.323 IP phones) Applications
<input type="radio"/> 2	Skype	Highest	Skype Applications
<input type="radio"/> 3	Netgear EVA	Highest	Netgear EVA Applications
<input type="radio"/> 4	Vonage IP Phone	Highest	Vonage IP Phone Applications
<input type="radio"/> 5	Google Talk	Highest	Google Talk Applications
<input type="radio"/> 6	MSN Messenger	High	MSN Messenger Applications
<input type="radio"/> 7	Yahoo Messenger	High	Yahoo Messenger Applications
<input type="radio"/> 8	Netmeeting (port 1720)	High	Netmeeting (port 1720) Applications
<input type="radio"/> 9	AIM	High	AIM Applications
<input type="radio"/> 10	SlingStream	High	SlingStream Applications
<input type="radio"/> 11	SSH	High	SSH Applications
<input type="radio"/> 12	Telnet	High	Telnet Applications
<input type="radio"/> 13	VPN	High	VPN Applications
<input type="radio"/> 14	Counter Strike	High	On-line gaming Counter Strike
<input type="radio"/> 15	Age of Empires	High	On-line gaming Age of Empires
<input type="radio"/> 16	Everquest	High	On-line gaming Everquest
<input type="radio"/> 17	Quake 2	High	On-line gaming Quake 2
<input type="radio"/> 18	Quake 3	High	On-line gaming Quake 3
<input type="radio"/> 19	Unreal Tourment	High	On-line gaming Unreal Tourment
<input type="radio"/> 20	Warcraft	High	On-line gaming Warcraft
<input type="radio"/> 21	FTP	Normal	FTP Applications
<input type="radio"/> 22	SMTP	Normal	SMTP Applications
<input type="radio"/> 23	PPIive	Normal	PPIive Applications
<input type="radio"/> 24	WWW	Normal	WWW Applications
<input type="radio"/> 25	DNS	Normal	DNS Applications
<input type="radio"/> 26	ICMP	Normal	ICMP Applications
<input type="radio"/> 27	eMule/eDonkey	Low	eMule/eDonkey Applications
<input type="radio"/> 28	Kazaa	Low	Kazaa Applications
<input type="radio"/> 29	Gnutella	Low	Gnutella Applications
<input type="radio"/> 30	BT/Azureus	Low	BT/Azureus Applications

- Select the radio button next to the QoS policy that you want to view or change.
- Click the **Edit** button.

The QoS - Priority Rules screen displays.

- Change the policy settings.

For information about changing policy setting, see the following sections:

- [Create a QoS Rule for an Application or Online Game](#) on page 62
- [Create a QoS Rule for a Modem Router LAN Port](#) on page 64
- [Create a QoS Rule for a MAC Address](#) on page 64

- On the QoS - Priority Rules screen, click the **Apply** button.

Your changes are saved in the table on the QoS Setup screen.

➤ **To delete a QoS rule:**

1. Select **ADVANCED > Setup > QoS Setup**.

The QoS Setup screen displays.

2. Click the **Setup QoS rule** button.

All preconfigured QoS rules are displayed in a table, along with their priority (Highest, High, Normal, or Low) and a description.

3. Select the radio button next to the QoS policy that you want to delete.



**WARNING:**

**Do not click the Delete All button. If you do, *all* preconfigured and custom QoS rules are deleted.**

4. Click the **Delete** button.

The QoS policy is removed from the table.

### **Create a QoS Rule for an Application or Online Game**

➤ **To create a QoS policy for an application or online game:**

1. Select **ADVANCED > Setup > QoS Setup**.

The QoS Setup screen displays.

2. Click the **Setup QoS rule** button.

The existing QoS rules display.

3. Click the **Add Priority Rule** button.

The QoS - Priority Rules screen displays.

4. From the Priority Category menu, select either **Applications** or **On-line gaming**:

- **Applications.** The Applications menu lets you select existing applications, but scroll down to the bottom of the menu to select **Add a new application**.

The screen adjusts:

- **On-line gaming.** The On-line gaming menu lets you select existing games, but scroll down to the bottom of the menu to select **Add a new game**.

The screen adjusts:

5. In the QoS Policy for field, type a descriptive name for the new application or game.
6. From the Priority menu, select the priority that this traffic needs to receive relative to other applications and traffic when accessing the Internet:

Select **Highest**, **High**, **Normal**, or **Low**.

7. In the Connection Type field, select either **TCP**, **UDP**, or **TCP/UDP**.
8. In the Starting Port and Ending Port fields, specify the port number or range of port numbers that is used by the application or game.
9. On the QoS - Priority Rules screen, click the **Apply** button.

The rule is saved in the QoS Policy table on the QoS Setup screen.

### Create a QoS Rule for a Modem Router LAN Port

- To create a QoS policy for a device connected to one of the modem router's LAN ports:

1. Select **ADVANCED > Setup > QoS Setup**.

The QoS Setup screen displays.

2. Click the **Setup QoS rule** button.

The existing QoS rules display.

3. Click the **Add Priority Rule** button.

The QoS - Priority Rules screen displays.

4. From the Priority Category menu, select **Ethernet LAN Port**.

The screen adjusts:

5. From the Ethernet LAN Port menu, select the LAN port (1, 2, 3, or 4) for which you want to configure the QoS policy.

The QoS Policy for field is automatically completed.

6. From the Priority menu, select the priority that this traffic needs to receive relative to other applications and traffic when accessing the Internet:

Select **Highest**, **High**, **Normal**, or **Low**.

7. On the QoS - Priority Rules screen, click the **Apply** button.

The rule is saved in the QoS Policy table on the QoS Setup screen.

### Create a QoS Rule for a MAC Address

- To create a QoS policy for traffic from a specific MAC address:

1. Select **ADVANCED > Setup > QoS Setup**.

The QoS Setup screen displays.

2. Click the **Setup QoS rule** button.

The existing QoS rules display.

3. Click the **Add Priority Rule** button.

The QoS - Priority Rules screen displays.



- From the Priority Category menu, select **MAC Address**.

The screen adjusts:

QoS - Priority Rules

Cancel Apply

**Priority**

QoS Policy for

Priority Category: MAC Address

**MAC Device List**

	QoS Policy	Priority	Device Name	MAC Address
<input type="radio"/>	Pri_MAC_ACAA5	Normal	VOSTRO1500	00:1D:09:AC:AA:7E

MAC Address

Device Name

Priority: Normal

+ Add Edit Delete Refresh

- In the QoS Policy for field, type a descriptive name for the new policy.
- If the device for which you want to create a QoS policy is displayed in the MAC Device List, select its radio button.

The information from the MAC Device List populates the QoS Policy (that is, the policy name), MAC Address, and Device Name fields.

- (Optional) If the device does not display in the MAC Device List, click the **Refresh** button. If it still does not display, complete the QoS Policy (that is, the policy name), MAC Address, and Device Name fields manually.
- From the Priority menu, select the priority that this traffic needs to receive relative to other applications and traffic when accessing the Internet:

Select **Highest**, **High**, **Normal**, or **Low**.

- On the QoS - Priority Rules screen, click the **Apply** button.

The rule is saved in the QoS Policy table on the QoS Setup screen.

➤ **To edit a MAC address on the MAC Device List:**

- Select **ADVANCED > Setup > QoS Setup**.  
The QoS Setup screen displays.
- Click the **Setup QoS rule** button.  
The existing QoS rules display.
- Click the **Add Priority Rule** button.  
The QoS - Priority Rules screen displays.
- From the Priority Category menu, select **MAC Address**.  
The MAC Device List displays.

5. Select the radio button next to the device that you want to change.
6. Change the MAC address, device name, or priority.
7. Click the **Edit** button.

**Note:** *You cannot edit a device that was detected by the modem router and automatically added to the MAC Device List.*

The device information is saved in the MAC Device List.

➤ **To remove a MAC address from the MAC Device List:**

1. Select **ADVANCED > Setup > QoS Setup**.

The QoS Setup screen displays.

2. Click the **Setup QoS rule** button.

The existing QoS rules display.

3. Click the **Add Priority Rule** button.

The QoS - Priority Rules screen displays.

4. From the Priority Category menu, select **MAC Address**.

The MAC Device List displays.

5. Select the radio button next to the device that you want to remove.
6. Click the **Delete** button.

**Note:** *You cannot remove a device that was detected by the modem router and automatically added to the MAC Device List.*

The device information is removed from the MAC Device List.

## Bandwidth Control

Bandwidth control lets you set a limit to the bandwidth that is available for traffic from the modem router to the Internet.

➤ **To set the maximum uplink bandwidth:**

1. Select **ADVANCED > Setup > QoS Setup**.

2. Select the **Turn Bandwidth Control On** check box.
3. Select the **Automatically check Internet Uplink bandwidth** radio button.
4. Click the **Check** button.

The modem router detects the available uplink bandwidth. After about one minute, the available bandwidth displays onscreen. This information can help you to determine the maximum bandwidth setting that you want to allow.

5. Select the **Uplink bandwidth** radio button.
6. Enter the maximum bandwidth that you want to allow.
7. Select either **Kbps** or **Mbps**.
8. Click the **Apply** button.

Your settings are saved.

# 5. Security

---

# 5

## Keep unwanted content out of your network

This chapter explains how to use the basic firewall features of the modem router to prevent objectionable content from reaching the computers and devices on your network.

This chapter includes the following sections:

- *Keyword Blocking of HTTP Traffic*
- *Set Up Firewall Rules to Control Network Access*
- *Add Custom Services to Allow or Block*
- *Schedule When to Block the Internet*
- *Security Event Email Notifications*

---

**Note:** For information about Live Parental Controls, see *Parental Controls* on page 34.

---

## Keyword Blocking of HTTP Traffic

Use keyword blocking to prevent certain types of HTTP traffic from accessing your network. By default, keyword blocking is disabled. The blocking can be always or according to a schedule.

➤ **To set up keyword blocking:**

1. Select **ADVANCED > Security > Block Sites**.

2. Select one of the keyword blocking options:
  - **Per Schedule.** Turn on keyword blocking according to the Schedule screen settings. For more information, see *Schedule When to Block the Internet* on page 76.
  - **Always.** Turn on keyword blocking all the time, independent of the Schedule screen.
3. In the Keyword field, enter a keyword or domain.
 

Here are some sample entries:

  - Specify XXX to block `http://www.badstuff.com/xxx.html`.
  - Specify .com if you want to allow only sites with domain suffixes such as .edu or .gov.
  - Enter a period (.) to block all Internet browsing access.
4. Click the **Add Keyword** button.
5. To add more keywords or domains, repeat *Step 3* and *Step 4*.
 

The keyword list supports up to 32 entries.

6. Click the **Apply** button.

Your settings are saved.

➤ **To delete a keyword or domain:**

1. Select **ADVANCED > Security > Block Sites**.

The Block Sites screen displays.

2. From the keyword list, select the keyword or domain that you want to remove.
3. Click the **Delete Keyword** button.
4. Click the **Apply** button.

Your settings are saved.

➤ **To remove all keywords and domains:**

1. Select **ADVANCED > Security > Block Sites**.

The Block Sites screen displays.

2. Click the **Clear List** button.
3. Click the **Apply** button.

Your settings are saved.

You can exempt one trusted computer from blocking and logging. The computer you exempt needs to have a fixed (static) IP address.

➤ **To specify a trusted computer:**

1. Select **ADVANCED > Security > Block Sites**.

The Block Sites screen displays.

2. In the Trusted IP Address field, enter the IP address of the trusted computer.

The first three octets of the IP address are automatically populated and depend on the IP address that is assigned to the modem router on the LAN Setup screen.

3. Click the **Apply** button.

Your settings are saved.

## Set Up Firewall Rules to Control Network Access

Your modem router has a firewall that blocks unauthorized access to your wireless network and permits authorized inbound and outbound communications. Authorized communications are established according to inbound and outbound rules. The firewall has the following two default rules:

- **Inbound.** Block all access from outside except responses to requests from the LAN side.
- **Outbound.** Allow all access from the LAN side to the outside.

You can add rules to further restrict the outbound communications or more widely open the inbound communications. Exceptions can be based on the service or application, source or destination IP addresses, and time of day. You can log traffic that matches or does not match the rule and change the order of rule precedence.

Traffic attempting to pass through the firewall is subjected to the rules in the order shown in the Rules table from the top (highest precedence) to the bottom. In some cases, the order of precedence determines which communications are allowed into or out of the network.

The Firewall Rules screen lists all firewall rules that you have added.

- To add a firewall rule for outbound traffic, see the following section, *Manage Outbound Firewall Rules*.
- To add a custom service that can be used in a firewall rule for outbound traffic, see *Add Custom Services to Allow or Block* on page 74.
- To add or change firewall rules for inbound traffic, see *Set Up Port Forwarding to Local Servers* on page 111 and *Set Up and Manage Port Triggering* on page 114.

After you have added outbound firewall rules, you can specify the days and time that you want to block Internet access. For more information, see *Schedule When to Block the Internet* on page 76.

## Manage Outbound Firewall Rules

By default, the firewall allows all access from the LAN side to the outside. You can set up rules to restrict access to particular services or applications and to restrict particular source or destination IP addresses.

---

**Note:** You cannot change or delete the default outbound firewall rule.

---

➤ **To add an outbound firewall rule:**

1. Select **ADVANCED > Security > Firewall Rules**.

The screenshot shows the 'Firewall Rules' configuration interface. At the top, there are 'Cancel' and 'Apply' buttons. Below is the 'Service Table' section with a table header for '#', 'Service Type', and 'Ports', and buttons for '+ Add Custom Service', 'Edit Service', and 'Delete Service'. The 'Outbound Services' section contains a table with columns for '#', 'Enable', 'Service Type', 'Action', 'LAN Users', 'WAN Servers', and 'Log'. A single 'Default' rule is listed with 'Enable' set to 'Yes', 'Service Type' as 'Any', 'Action' as 'ALLOW always', 'LAN Users' as 'Any', 'WAN Servers' as 'Any', and 'Log' as 'Never'. Below this table are buttons for '+ Add', 'Edit', and 'Delete'. The 'Inbound Services' section at the bottom includes a link: 'Click [here](#) to set up inbound Firewall Rules for gaming or other applications.'

- In the Outbound Services section, click the **Add** button.

- Select the service or application to be covered by this rule.

If the service or application that you want does not display in the menu, you can define it (see [Add Custom Services to Allow or Block](#) on page 74).

- Select the action you want for traffic covered by this rule:

- **BLOCK always.** Always block the traffic covered by this rule.
- **BLOCK by schedule, otherwise Allow.** Allow the traffic covered by this rule, unless it is blocked according to the schedule specified on the Schedule screen (see [Schedule When to Block the Internet](#) on page 76).
- **ALLOW always.** Always allow the traffic covered by this rule (this selection is the default setting).
- **ALLOW by schedule, otherwise Block.** Block the traffic covered by this rule, unless it is blocked according to the schedule specified on the Schedule screen (see [Schedule When to Block the Internet](#) on page 76).

**Note:** *ALLOW rules are useful only when the traffic is already covered by a BLOCK rule. Use these rules when you want to allow a subset of traffic that is blocked by another rule.*

- Specify which computers on your network are affected by this rule, based on their source (LAN) IP address:
  - **Any.** All local IP addresses are covered by this rule.
  - **Single address.** Type the required address in the Start field.
  - **Address range.** Type the start address for the range in the Start field and the end address for the range in the End field.
- Specify which Internet locations are covered by the rule, based on their destination (WAN) IP address:
  - **Any.** All Internet IP addresses are covered by this rule.



- **Single address.** Type the required address in the Start field.
  - **Address range.** Type the start address for the range in the Start field and the end address for the range in the End field.
7. Specify whether traffic covered by this rule is logged:
- **Never.** The modem router never logs traffic covered by this rule, whether it matches or not.
  - **Always.** The modem router logs traffic that is covered by this rule, whether it matches or not.

Logging can be useful when you are debugging your rules.

8. Click the **Add** button.

The new firewall rule is added to the Outbound Services table on the Firewall Rules screen. The firewall rule is enabled by default.

➤ **To disable an existing outbound firewall rule:**

1. Select **ADVANCED > Security > Firewall Rules**.

The Firewall Rules screen displays.

2. In the Outbound Services table, clear the **Enable** check box for the firewall rule that you want to disable.

3. Click the **Apply** button.

Your settings are saved.

➤ **To change an existing outbound firewall rule:**

1. Select **ADVANCED > Security > Firewall Rules**.

The Firewall Rules screen displays.

2. In the Outbound Services table, select the radio button to the left of the firewall rule that you want to change.

3. Click the **Edit** button.

The Block Services Setup screen displays. This screen has the same fields as the Outbound Firewall Rule screen on which you can set up a new firewall rule.

4. Change the settings of the firewall rule.

5. Click the **Accept** button.

The changed settings of the firewall rule are shown in the Outbound Services table on the Firewall Rules screen. The firewall rule is enabled by default.

➤ **To remove an existing outbound firewall rule:**

1. Select **ADVANCED > Security > Firewall Rules**.

The Firewall Rules screen displays.

2. In the Outbound Services table, select the radio button to the left of the firewall rule that you want to remove.

3. Click the **Delete** button.

The firewall rule is removed from the Outbound Services table on the Firewall Rules screen.

## Manage Inbound Firewall Rules

By default, the firewall blocks all access from outside except responses to requests from the LAN side. You can set up rules to allow access to particular services, applications, ports, and computers. These rules are implemented through port forwarding and port triggering.

### ➤ To add an inbound firewall rule:

1. Select **ADVANCED > Security > Firewall Rules**.

The Firewall Rules screen displays.

2. In the Inbound Services section, click the **here** link.

You are redirected to the Port Forwarding / Port Triggering screen. For more information, see *Set Up Port Forwarding to Local Servers* on page 111 and *Set Up and Manage Port Triggering* on page 114.

## Add Custom Services to Allow or Block

You can define your own incoming and outgoing custom services to allow or block. Once you add your own custom services, they are available on the Outbound Firewall Rule screen (see *Manage Outbound Firewall Rules* on page 71).

Before you add a custom service, first determine which port number or range of numbers is used by the service or application. You can usually determine this information by contacting the publisher of the application or the user groups or news groups.

### ➤ To add a custom service:

1. Select **ADVANCED > Security > Firewall Rules**.



Firewall Rules

Cancel Apply

Service Table

#	Service Type	Ports
+ Add Custom Service	Edit Service	Delete Service

Outbound Services

#	Enable	Service Type	Action	LAN Users	WAN Servers	Log
Default	Yes	Any	ALLOW always	Any	Any	Never

+ Add Edit Delete

Inbound Services  
Click [here](#) to set up inbound Firewall Rules for gaming or other applications.

- In the Service Table section, click the **Add Custom Service** button.

- In the Service Type/User Defined field, type a suitable name for the new service or application.
- From the Protocol menu, select the correct type of protocol for the new service:
  - TCP**
  - UDP**
  - TCP/UDP**

**Note:** *If you are not sure which protocol to select, select **TCP/UDP**.*

- In the Starting Port field, enter the starting port number for the new service or application.
- In the Ending Port field, enter the ending port number for the new service or application.  
If the service or application uses a single port number, enter that number in both fields.
- Click the **Add** button.

The new service or application is added to the Services Table on the Firewall Rules screen.

➤ **To change an existing custom service:**

- Select **ADVANCED > Security > Firewall Rules**.

The Firewall Rules screen displays.

- In the Service Table, select the radio button to the left of the service that you want to change.
- Click the **Edit Service** button.

The Add Services screen displays.

- Change the settings for the service or application.
- Click the **Accept** button.

The changed settings of the custom service are shown in the Service Table on the Firewall Rules screen.

➤ **To remove an existing custom service:**

- Select **ADVANCED > Security > Firewall Rules**.

The Firewall Rules screen displays.

2. In the Service Table, select the radio button to the left of the service that you want to remove.
3. Click the **Delete Service** button.

The custom service is removed from the Service Table on the Firewall Rules screen.

## Schedule When to Block the Internet

After you have added keyword blocking (see *Keyword Blocking of HTTP Traffic* on page 69), outbound firewall rules (see *Set Up Firewall Rules to Control Network Access* on page 70), or both, you can specify the days and time that you want to block Internet access.

By default, there is no schedule and Internet access is blocked according to the keywords that you have specified and the outbound firewall rules that you have added.

### ➤ To schedule blocking:

1. Select **ADVANCED > Security > Schedule**.

The screenshot shows the 'Schedule' configuration window. At the top, there are 'Cancel' and 'Apply' buttons. Below the title bar, the 'Days to Block' section has checkboxes for 'Every Day', 'Sunday', 'Monday', 'Tuesday', 'Wednesday', 'Thursday', 'Friday', and 'Saturday', all of which are checked. The 'Time of day to block' section includes an 'All Day' checkbox (checked) and two rows of time selection: 'Start Blocking' (0 Hour, 0 Minute) and 'End Blocking' (24 Hour, 0 Minute). The 'Time Zone' section has a dropdown menu set to '(GMT-08:00) Pacific Time (US & Canada): Tijuana' and an unchecked checkbox for 'Automatically adjust for daylight savings time'. At the bottom, the 'Current Time' is displayed as 'Tuesday, Jan 01, 2013 07:46:42'.

2. Set up the schedule for blocking keywords and services.
  - **Days to Block.** Select days on which you want to apply blocking by selecting the appropriate check boxes, or select the **Every Day** check box to select the check boxes for all days.
  - **Time of Day to Block.** Select a start and end time in 24-hour format, or select the **All Day** check box for 24-hour blocking.
3. Select your time zone from the Time Zone menu.
4. If you use daylight saving time, select the **Automatically adjust for daylight savings time** check box.

- Click the **Apply** button.

Your settings are saved.

## Security Event Email Notifications

To receive logs and alerts by email, provide your email information in the E-mail screen, and specify which alerts you want to receive and how often.

- **To set up email notifications:**

- Select **ADVANCED > Security > E-mail**.

- Select the **Turn Email Notification On** check box.
- In the Your Outgoing Mail Server field, enter the name of your ISP's outgoing (SMTP) mail server (such as mail.myISP.com).

You might be able to find this information in the configuration screen of your email program. If you leave this field blank, log and alert messages are not sent.

- Enter the email address to which logs and alerts are sent in the Send to This Email Address field.

This email address is also used for the From address. If you leave this field blank, log and alert messages are not sent.

- If your outgoing email server requires authentication, set up the authentication:
  - Select the **My Mail Server requires authentication** check box.
  - Fill in the User Name and Password fields for the outgoing email server.
- (Optional) Select the **Send Alerts Immediately** check box.

Email alerts are sent immediately when someone attempts to visit a blocked site.

7. (Optional) Select when logs are sent automatically:

a. Select an option from the menu:

- **When log is full**
- **Hourly**
- **Daily**
- **Weekly**
- **None**

b. If you select Daily or Weekly, select the time from the menu, and select the **a.m.** or **p.m.** radio button.

c. If you select Weekly, select the day from the menu.

Logs are sent automatically. If the log fills up before the specified time, the log is emailed. After the log is sent, the log is cleared from the modem router memory. If the modem router cannot email the log file, the log buffer might fill up. In this case, the modem router overwrites the log and discards its contents.

8. Click the **Apply** button.

Your settings are saved.

# 6 Administration

---

# 6

## Manage your network

This chapter describes the modem router settings for administering and maintaining your modem router and home network.

This chapter includes the following sections:

- [Update the Modem Router Firmware](#)
- [View Router Status](#)
- [View and Manage the Logs](#)
- [Manage the Configuration File](#)
- [Change the Password](#)
- [Password Recovery](#)
- [Perform Diagnostics](#)

For information about other administrative tasks, see the following sections:

- For information about viewing attached devices, see [View Attached Devices](#) on page 44.
- For information about upgrading or checking the status of your modem router over the Internet, see [Remote Management](#) on page 121.
- For information about monitoring Internet traffic, See [Traffic Meter](#) on page 134.

## Update the Modem Router Firmware

The modem router firmware (routing software) is stored in flash memory. You can update the firmware from the Administration menu on the ADVANCED tab. You might see a message at the top of the genie screens when new firmware is available for your product.

You can use the Check button on the Router Update screen to check and update to the latest firmware for your product if new firmware is available.

➤ **To check for new firmware and update your modem router:**

1. Select **ADVANCED > Administration > Router Update**.

2. Click the **Check** button.

The modem router finds new firmware information if any is available.

3. Click the **Yes** button.

The modem router locates the firmware that you downloaded and begins the update. The firmware file ends in .img.

4. (Optional) If you have manually downloaded new firmware from the NETGEAR support website:

- a. Click the **Browse** button, navigate to the firmware file (the file ends in .img), and select the firmware file.

- b. Click the **Upload** button.

A progress bar shows the progress of the firmware upload process.



**WARNING:**

**To avoid the risk of corrupting the firmware, do not interrupt the upload. For example, do not close the browser, click a link, or load a new page. Do not turn off the modem router.**

When the upload is complete, your modem router restarts. The firmware update process typically takes about three minutes.



➤ **To download new firmware manually and update your modem router:**

1. Visit [downloadcenter.netgear.com](http://downloadcenter.netgear.com), locate the DGN1000Bv3 support page, and download the new firmware.
2. Read the new firmware release notes to determine whether you must reconfigure the modem router after upgrading.
3. Select **ADVANCED > Administration > Router Update**.

The screenshot shows a web interface for firmware updates. At the top, it says 'Firmware Update'. Below that, there's a section titled 'Check for new version from the Internet.' with a blue 'Check' button. Underneath, there's another section titled 'Locate and select the upgrade file on your hard disk.' which includes a text input field and a 'Browse...' button. At the bottom of the interface, there are two buttons: a blue 'Cancel' button and a green 'Upload' button with a right-pointing arrow.

4. Locate and select the firmware file on your computer:
  - a. Click the **Browse** update.
  - b. Navigate to the firmware file.  
The file ends in .img.
  - c. Select the firmware file.
5. Click the **Upload** button.

A progress bar shows the progress of the firmware upload process.



**WARNING:**

**To avoid the risk of corrupting the firmware, do not interrupt the upload. For example, do not close the browser, click a link, or load a new page. Do not turn off the modem router.**

When the upload is complete, your modem router restarts. The firmware update process typically takes about three minutes.

## View Router Status

- To view modem router status and usage information:

Depending on the screen that you have open, select **ADVANCED** or **ADVANCED Home**:

The screenshot shows the 'ADVANCED' status page of the N150 Wireless ADSL2+ Modem Router. The interface includes a sidebar with navigation options and several main content panels.

**Router Information**

Hardware Version	DGN1000v3-A
Firmware Version	V1.0.0.4_0.0.4AU
GUI Language Version	V1.0.0.7

**LAN Port**

MAC Address	28:C6:8E:AD:BC:2E
IP Address	192.168.0.1
DHCP Server	On

**Internet Port**

MAC Address	28:C6:8E:AD:BC:2F
IP Address	10.0.0.15
Connection	PPPoE
IP Subnet Mask	255.255.255.255
Domain Name Server	203.0.113.1 203.0.113.2

**Modem**

xDSL Firmware Version	4925ca26
Modem Status	connected
DownStream Connection Speed	24044
UpStream Connection Speed	1138
VPI	8
VCI	38

**Wireless Settings**

Name (SSID)	NETGEAR51
Region	United States
Channel	Auto ( 1 )
Mode	Up to 65 Mbps
Wireless AP	On
Broadcast Name	On
Wireless isolation	Off
Wi-Fi Protected Setup	Configured

**Guest Network**

Name (SSID)	NETGEAR-Guest1
Wireless AP	Off
Broadcast Name	On
Wireless isolation	Off
Allow guest to access My Local Network	Off

## Router Information

The following settings are displayed:

- **Hardware Version.** The modem router model.
- **Firmware Version.** The version of the modem router firmware. It changes if you update the modem router firmware.
- **GUI Language Version.** The localized language of the web management interface.
- **LAN Port.**
  - **MAC Address.** The Media Access Control address. This is the unique physical address used by the Ethernet (LAN) port of the modem router.
  - **IP Address.** The IP address used by the Ethernet (LAN) port of the modem router. The default is 192.168.0.1.
  - **DHCP Server.** Identifies whether the modem router's built-in DHCP server is active for devices on the LAN.

➤ **To reboot the modem router:**

Click the **Reboot** button.

## Internet Port

The following settings are displayed:

- **MAC Address.** The Media Access Control address, which is the unique physical address used by the Internet (WAN) port of the modem router.
- **IP Address.** The IP address used by the Internet (WAN) port of the modem router. If no address is shown or the address is 0.0.0.0, the modem router cannot connect to the Internet.
- **Connection.** This field shows if the modem router is using a fixed IP address on the WAN. If the value is DHCP Client, the modem router obtains an IP address dynamically from the ISP.
- **IP Subnet Mask.** The IP subnet mask used by the Internet (WAN) port of the modem router.
- **Domain Name Server.** The Domain Name Server addresses used by the modem router. A Domain Name Server translates human-language URLs such as www.netgear.com into IP addresses.

## Statistics Screen

### ➤ To view statistics:

1. Depending on the screen that you have open, select **ADVANCED** or **ADVANCED Home**.
2. In the Internet Port pane, click the **Show Statistics** button.

System Up Time 02:58:07							
Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	Link Down	0	0	0	0	0	00:00:00
LAN 1	Link Down	18584	12990	0	1439	113	00:00:00
LAN 2	Link Down						00:00:00
LAN 3	Link Down						00:00:00
LAN 4	100M/Full						02:53:32
WLAN	54M	505	517	0	13	5	01:02:46

Poll Interval:  (secs) Set Interval Stop

The following information is displayed:

- **System Up Time.** The time elapsed since the modem router was last restarted.
- **Port.** The statistics for the WAN (Internet), four LAN (Ethernet) ports, and WLAN (wireless LAN) port. For each port, the screen displays:
  - **Status.** The link status of the port.
  - **TxPkts.** The number of packets transmitted on this port since reset or manual clear.
  - **RxPkts.** The number of packets received on this port since reset or manual clear.
  - **Collisions.** The number of collisions on this port since reset or manual clear.
  - **Tx B/s.** The current transmission (outbound) bandwidth used on the WAN and LAN ports.
  - **Rx B/s.** The current reception (inbound) bandwidth used on the WAN and LAN ports.
  - **Up Time.** The time elapsed since this port acquired the link.
- **Poll Interval.** The interval at which the statistics are updated in this screen.

### ➤ To change the polling frequency:

1. In the Poll Interval field, enter a time in seconds.
2. Click the **Set Interval** button.

### ➤ To stop the polling:

Click the **Stop** button.

## Connection Status Screen

### ➤ To view and change the Internet connection status:

1. Depending on the screen that you have open, select **ADVANCED** or **ADVANCED Home**.

- In the Internet Port pane, click the **Connection Status** button.

Connection Status	
Connection Time	00:00:00
Connection Status	disconnected
Negotiation	----
Authentication	----
IP Address	0.0.0.0
Subnet Mask	0.0.0.0

The following information displays:

- **Connection Time.** The time elapsed since the last connection to the Internet through the DSL port.
  - **Connection Status.** Connected or disconnected.
  - **Negotiation.** ---- (which indicates off) or Successful.
  - **Authentication.** ---- (which indicates off) or Successful.
  - **IP Address.** The IP address that is assigned to the modem router.
  - **Subnet Mask.** The subnet mask that is assigned to the modem router.
- (Optional) Connect or disconnect the modem router from the Internet.
    - Click the **Connect** button.
    - Click the **Disconnect** button.

➤ **To close the Connection Status screen:**

Click the **Close Window** button.

## Modem

The following settings are displayed:

- **xDSL Firmware Version.** The firmware version is displayed for information only. You cannot manage the xDSL firmware.
- **Modem Status.** Connected, disconnected, or system crash.
- **DownStream Connection Speed.** The downstream connection speed that the modem router detected.
- **UpStream Connection Speed.** The upstream connection speed that the modem router detected.
- **VPI.** The VPI that you configured on the xDSL Setup screen, or the default VPI, which is 0.
- **VCI.** The VCI that you configured on the xDSL Setup screen, or the default VCI, which is 38.

➤ **To view the modem statistics:**

Click the **Modem Statistics** button.

xDSL Line Status		
Mode		
Latency		
Trellis Coding	Enable	
Status	ACTIVATING.	
Power Level	L0	
Uptime	0	
	Downstream	Upstream
SNR Margin (dB)	0.0	0.0
Attenuation (dB)	0.0	0.0
Output Power (dBm)	0.0	0.0
Attainable Rate (Kbps)	0	0
Rate (kbps)	0	0
K (number of bytes in DMT frame)		
R (number of check bytes in RS code word)		
S (RS code word size in DMT frame)		
D (interleave depth)		
Delay (msec)		
FEC	0	0
CRC	0	0
Total ES	0	0
Total SES	0	0
Total UAS	0	0
Total LOSS	--	--
Full Init	0	
Failed Full Init	0	
Last Link DS Rate	0	
Last Link US Rate	0	
TX frames	0	
RX frames	0	
Synchronized time (Second)		
Synchronized number	0	
<a href="#">Close Window</a>		

The information that is displayed on this screen is not described in this manual. This information is typically used by NETGEAR support.

➤ **To close the xDSL Line Status screen:**

Click the **Close Window** button.

## Wireless Settings

The following settings are displayed:

- **Name (SSID).** The wireless network name (SSID) that the modem router uses.
- **Region.** The geographic region where the modem router is being used. It might be illegal to use the wireless features of the modem router in some parts of the world.
- **Channel.** The operating channel of the wireless port being used. The default channel is Auto. When Auto is selected, the modem router finds the best operating channel available.
- **Mode.** The wireless mode: Up to 54 Mbps, Up to 65 Mbps (default), or Up to 150 Mbps.
- **Wireless AP.** Indicates On or Off to specify if the radio feature of the modem router is enabled. If this feature is not enabled, the Wireless LED on the front panel is off.
- **Broadcast Name.** Indicates On or Off to specify if the modem router is broadcasting its SSID.
- **Wireless isolation.** Indicates On or Off to specify if wireless isolation prevents wireless clients from communicating with each other when they join the wireless network.
- **Wi-Fi Protected Setup.** Indicates whether WPS is configured for this network.

## Guest Network

The following settings are displayed:

- **Name (SSID).** The wireless network name (SSID) used by the modem router for the guest network. The default names are NETGEAR-Guest1, NETGEAR-Guest2, and NETGEAR-Guest3. If all guest networks are active at the same time, the screen shows only NETGEAR-Guest1.
- **Wireless AP.** Indicates On or Off to specify if the radio feature is enabled for any guest network.
- **Broadcast Name.** Indicates On or Off to specify if the modem router is broadcasting the SSID for the guest network.
- **Wireless Isolation.** Indicates On or Off to specify if wireless isolation prevents wireless clients from communicating with each other when they join the guest network.
- **Allow guest to access My Local Network.** Indicates On or Off to specify if a user who connects to the guest network can access the local network that is associated with the modem router.

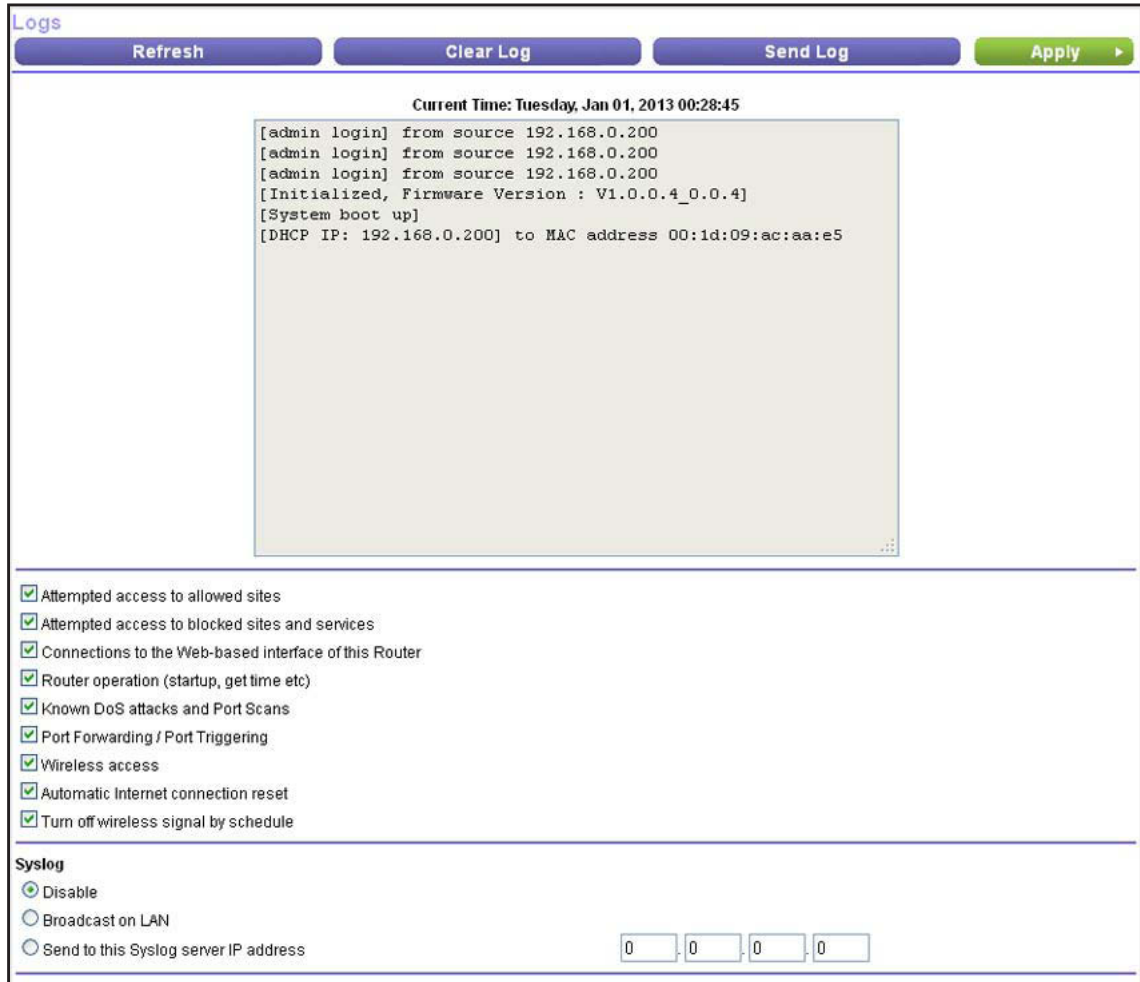
## View and Manage the Logs

The log is a detailed record of websites that users have accessed or attempted to access, modem router operation, DoS attacks and port scans, wireless access, and other information. Up to 256 entries are stored in the log.

You can specify which types of actions and events are logged, and how the system logs are sent. By default, all actions and events are logged, and the system logs are not sent anywhere.

➤ **To view logs:**

Select **ADVANCED > Administration > Logs**.



Depending on the type of action that was logged, the log screen can show the following information:

- **Action.** Whether access was blocked or allowed, whether a service was initialized, whether a user logged in, and so on.
- **Source IP.** The IP address of the initiating device for this log entry.
- **Target address.** The name or IP address of the website or news group that a user visited or attempted to access, the IP address from which a DoS or port scan was initiated, the IP address from which time was synchronized, the MAC address to which the DHCP server issues an IP address, and so on.
- **Date and time.** The date and time the log entry was recorded.



➤ **To refresh the log screen:**

Click the **Refresh** button.

➤ **To clear the log entries:**

Click the **Clear Log** button.

➤ **To email the log immediately:**

Click the **Send Log** button.

**Note:** *To send and receive emails, make sure that you have set up and enabled email notification (see [Security Event Email Notifications](#) on page 77).*

## Change Which Actions and Events Are Logged

➤ **To configure which actions are logged:**

**1.** Select **ADVANCED > Administration > Logs**.

The Logs screen displays.

**2.** Select or clear any of the following check boxes:

- **Attempted access to allowed sites.** Log attempts to access websites that are allowed.
- **Attempted access to blocked sites and services.** Log attempts to access websites and services that are blocked.
- **Connections to the Web-based interface of this Router.** Log access to the modem router web management interface.
- **Router operation (startup, get time etc).** Log modem router operation events such as startup, Internet connection, firmware initialization, and time synchronization.
- **Known DoS attacks and Port Scans.** Log DoS attacks and port scans.
- **Port Forwarding / Port Triggering.** Log port forwarding and port triggering events.
- **Wireless access.** Log access by wireless clients.
- **Automatic Internet connection reset.** Log when the Internet connection is reset automatically.
- **Turn off wireless signal by schedule.** Log when the radio is turned off if the wireless signal is scheduled to be turned off.

By default, all of these check boxes are selected.

**3.** Click the **Apply** button.

Your settings are saved.

## Set Up How the System Logs Are Sent

By default, no system logs (syslogs) are sent. Before you set up where the system logs are sent, set up when system logs are sent and enable email notification (see *Security Event Email Notifications* on page 77).

➤ **To set up where system logs are sent:**

1. Select **ADVANCED > Administration > Logs**.

The Logs screen displays.

2. Specify where system logs are sent by selecting one of the following check boxes:
  - **Broadcast on LAN.** The system logs are sent to the broadcast IP address (255.255.255.255) on the LAN.
  - **Send to this Syslog server IP address.** The system logs are sent to the syslog server that you need to specify in the IP address fields.
3. Click the **Apply** button.

Your settings are saved.

## Manage the Configuration File

The configuration settings of the modem router are stored within the modem router in a configuration file. You can back up (save) this file to your computer, restore it, or reset it to the factory default settings.

### Back Up Settings

➤ **To back up the modem router's configuration settings:**

1. Select **ADVANCED > Administration > Backup Settings**.

The screenshot shows the 'Backup Settings' page. It has a title bar 'Backup Settings'. Below it, there are three main sections separated by horizontal lines. The first section is 'Save a copy of current settings' with a blue 'Back Up' button. The second section is 'Restore saved settings from a file' with a text input field, a 'Browse...' button, and a blue 'Restore' button. The third section is 'Revert to factory default settings' with a blue 'Erase' button.

2. Click the **Back Up** button.
3. Choose a location to store the .cfg file that is on a computer on your network.  
A copy of the current settings is saved.

## Restore Configuration Settings

➤ **To restore configuration settings that you backed up:**

1. Select **ADVANCED > Administration > Backup Settings**.

The Backup Settings screen displays.

2. Click the **Browse** button.
3. Locate and select the .cfg file.
4. Click the **Restore** button.

The file is uploaded to the modem router, and the modem router reboots.



**WARNING:**

**Do not interrupt the reboot process.**

## Erase the Current Configuration Settings

You can use the Erase button to erase the configuration and restore the factory default settings. You might want to erase the configuration if you move the modem router to a different network.

You can also use the Restore Factory Settings button on the right side panel of the modem router to erase the configuration and restore the factory settings. For more information, see [Side Panel with Restore Factory Settings Button](#) on page 12 and [Factory Settings](#) on page 149.

➤ **To erase the configuration settings:**

1. Select **ADVANCED > Administration > Backup Settings**.

The Backup Settings screen displays.

2. Click the **Erase** button.

The factory default settings are restored. The user name is admin, the password is password, and the LAN IP address is 192.168.0.1. DHCP is enabled.

## Change the Password

This feature lets you change the default password that is used to log in to the modem router with the user name admin.

Changing the password is not the same as changing the password for wireless access. The label on the modem router shows your unique wireless network name (SSID) and password for wireless access (for more information, see [Bottom Panel](#) on page 13).

➤ **To change the password for the user name admin:**

1. Select **ADVANCED > Administration > Set Password**.

The screenshot shows the 'Set Password' configuration page. At the top, there are 'Cancel' and 'Apply' buttons. Below them are three input fields: 'Old Password', 'Set Password', and 'Repeat New Password'. A checkbox labeled 'Enable Password Recovery' is present. At the bottom, there is a field for 'Administrator login times out after idle for' with the value '5' and the unit 'minutes'.

2. Type the old password, and type the new password twice.
3. (Optional) Specify a value in minutes to change the automatic logout time.

By default, if you are logged in to the web management interface as an administrator and the web management interface remains idle for five minutes, you are logged out automatically.

4. Click the **Apply** button.

Your settings are saved.

## Password Recovery

NETGEAR recommends that you enable password recovery if you change the password for the user name admin. Then you can recover the password if it is forgotten. This recovery is supported in Internet Explorer, Firefox, and Chrome browsers, but not in the Safari browser.

➤ **To set up password recovery:**

1. Select **ADVANCED > Administration > Set Password**.

The Set Password screen displays.

2. Select the **Enable Password Recovery** check box.

The screen adjusts:

3. From the lists, select two security questions, and provide answers to them.
4. Click the **Apply** button.

Your settings are saved.

➤ **To recover your password:**

1. In the address field of your browser, type **www.routerlogin.net**.  
A login screen displays.
2. Click the **Cancel** button.  
If password recovery is enabled, you are prompted to answer two security questions.
3. Enter the saved answers to the security questions.

## Perform Diagnostics

You can perform two diagnostics tests:

- **Ping an IP address or Host Name.** Use this test to send a ping packet request to the specified IP address or host name.

This test is often used to test a connection. If the request times out (in other words, no reply is received), this result usually means that the destination is unreachable. Note, however, that some network devices can be configured not to respond to a ping.

- **Perform a DNS Lookup.** A DNS (Domain Name Server) converts the Internet name (for example, [www.netgear.com](http://www.netgear.com)) to an IP address.

If you need the IP address of a web, FTP, mail, or other server on the Internet, do a DNS lookup to find the IP address.

For normal operation, these tests are not required.

➤ **To perform diagnostic tests:**

1. Select **ADVANCED > Administration > Diagnostics**.

2. (Optional) Ping an IP address or host name:
  - a. Type an IP address or host name in the field.
  - b. Click the **Ping** button.  
The ping results display onscreen.
  - c. To return to the Diagnostics screen, click the **Back** button.

3. (Optional) Perform a DNS lookup:

- a. Type an Internet name in the field.
- b. Click the **Lookup** button.

The IP address displays, and the DNS Server field displays the primary and secondary DNS servers that were detected on the WAN.

➤ **To display the internal routing table:**

1. Select **ADVANCED > Administration > Diagnostics**.

The Diagnostics screen displays.

2. Click the **Display** button.

The internal routing table displays onscreen.

3. To return to the Diagnostics screen, click the **Back** button.

You can perform a remote restart of the modem router. Use this operation if the modem router seems to have become unstable or is not operating normally.

Rebooting breaks any existing connections either to the modem router (for example, a connection to the web management interface) or through the modem router (for example, LAN users accessing the Internet). However, connections to the Internet are automatically reestablished if possible.

➤ **To reboot the modem router:**

1. Select **ADVANCED > Administration > Diagnostics**.

The Diagnostics screen displays.

2. Click the **Reboot** button.

# 7. Advanced Settings

---

# 7

## Set up unique situations

This chapter describes the advanced features of your modem router. Networking knowledge is needed to implement some of these features.

This chapter includes the following sections:

- *Advanced Wireless Settings*
- *Wireless Distribution System*
- *Port Forwarding and Port Triggering*
- *Set Up Port Forwarding to Local Servers*
- *Set Up and Manage Port Triggering*
- *Dynamic DNS*
- *Static Routes*
- *Remote Management*
- *Universal Plug and Play*
- *IPv6*
- *Traffic Meter*



## Advanced Wireless Settings

You can use this screen to turn the wireless radio on and off, to configure advanced wireless settings, to specify WPS settings, to use AP mode, and to set up a wireless access list.

### Control the Wireless Radio

By default, the wireless radio is enabled so that you can connect wirelessly to the modem router. You can turn the wireless radio on or off on the Advanced Wireless Settings screen or by using the WiFi On/Off button on the modem router front panel. When the wireless radio is off, you can still use an Ethernet cable for a LAN connection to the modem router.

- **To turn the radio on or off and change advanced settings for your wireless network:**
  1. Select **ADVANCED > Advanced Setup > Wireless Settings**.

**Advanced Wireless Settings**

Enable Wireless Router Radio

Enable 20/40MHz Coexistence

Fragmentation Length (256-2346)

CTS/RTS Threshold (1-2347)

Preamble Mode

Transmit Power Control

Turn off wireless signal by schedule

The wireless signal is scheduled to turn off during the following time period:

Period	Start	End	Recurrence pattern

**WPS Settings**

Router's PIN: **10000571**

Enable Router's PIN

To prevent PIN compromise, auto disable the PIN after  failed PIN connections, until router reboots.  
In auto disabled mode, router's WPS LED will keep blinking slowly

Keep Existing Wireless Settings

**Wireless Card Access List**

By default, the Enable Wireless Router Radio check box is selected.

2. (Optional) Clear the **Enable Wireless Router Radio** check box.

Clearing this check box turns off the WiFi feature of the modem router. When the wireless radio is disabled, you can still use the modem router by connecting computers to the modem router with an Ethernet cable. By default, the wireless radio is enabled.

3. (Optional) Clear the **Enable 20/40 MHz Coexistence** check box.

By default, 20/40 MHz coexistence is enabled to prevent interference between wireless network in your environment at the expense of the wireless speed. If there are no other

wireless networks in your environments, you can clear the Enable 20/40 MHz Coexistence check box to increase the wireless speed to the maximum supported speed.



**WARNING:**

**The Fragmentation Length, CTS/RTS Threshold, and Preamble Mode options are reserved for wireless testing and advanced configuration only. Do not change these settings unless directed by NETGEAR support. Incorrect settings might disable the wireless function of the modem router unexpectedly.**

4. (Optional) Lower the wireless transmit power by selecting a value lower than 100% from the Transmit Power Control menu.

The setting of 100% allows the modem router to use the maximum wireless transmit power to transmit wireless packets. Reducing the transmit power can save the power consumption for the modem router but also reduces the wireless coverage. If you want to have maximum wireless coverage, NETGEAR recommends that you leave the setting on the Transmit Power Control menu at 100%.

5. Click the **Apply** button.

Your changes take effect.

## Set Up a Wireless Schedule

You can use this feature to turn off the wireless signal from your modem router at times when you do not need a wireless connection. For example, you might turn it off for the weekend if you leave town. You can create up to 20 wireless schedules.

---

**Note:** You can configure a wireless schedule only if the modem router obtained its network time. If you do not have a DSL or Internet connection, the modem router cannot reach a network time server, and you cannot configure a wireless schedule.

---

➤ **To configure and enable a wireless schedule:**

1. Select **ADVANCED > Advanced Setup > Wireless Settings**.

The Advanced Wireless Settings screen displays.

2. Click the **Add a new period** button.

The screen adjusts:

3. Use the menus, radio buttons, and check boxes to set up a period during which you want the wireless signal to be turned off.

The Start and End menus use 24-hour clock settings. Setting up a schedule is self-explanatory.

4. Click the **Apply** button.

Your settings are saved. The Advanced Wireless Settings screen displays.

5. Select the **Turn off wireless signal by schedule** check box to activate the schedule.

6. Click the **Apply** button.

Your settings are saved. The wireless schedule is added to the table on the Advanced Wireless Settings screen.

➤ **To change a wireless schedule:**

1. Select **ADVANCED > Advanced Setup > Wireless Settings**.

The Advanced Wireless Settings screen displays.

2. In the table, select the radio button next to the wireless Schedule for which you want to make a change.

3. Click the **Edit** button.

The screen adjusts.

4. Use the menus, radio buttons, and check boxes to modify the period during which you want the wireless signal to be turned off.

5. Click the **Apply** button.

Your settings are saved. The table on the Advanced Wireless Settings screen displays the modified wireless schedule.

➤ **To remove a wireless schedule:**

1. Select **ADVANCED > Advanced Setup > Wireless Settings**.

The Advanced Wireless Settings screen displays.

2. In the table, select the radio button next to the wireless Schedule that you want to remove.
3. Click the **Delete** button.

The wireless schedule is removed from the table on the Advanced Wireless Settings screen.

## View or Change WPS Settings

You can control how WPS functions on the modem router. NETGEAR recommends that you use caution if you change the WPS settings.

---

**Note:** For information about how to use WPS to add wireless devices and other equipment to your wireless network, see *WPS Wizard for WiFi Connections* on page 57.

---

You cannot set up the WPS settings when the security is WEP. Make sure that the security mode is WPA-PSK, WPA2-PSK, or WPA-PSK + WPA2-PSK mixed mode. For information about configuring the security mode, see *Basic Wireless Settings* on page 36.

You can do the following with the modem router's PIN:

- Disable the PIN entirely.
- Change the number of times that a PIN connection is allowed to fail before the PIN is automatically disabled. By default, the PIN is automatically disabled after three failed connection attempts. If the PIN is automatically disabled, it remains so until you restart the modem router. While the PIN is disabled, the WPS LED blinks slowly.
- Turn off automatic disabling of the PIN.

### ➤ To specify WPS settings:

1. Select **ADVANCED > Advanced Setup > Wireless Settings**.

The Advanced Wireless Settings screen displays.

The Router's PIN field displays the PIN that you use on a registrar (for example, from the Network Explorer on a Vista Windows computer) to configure the modem router's wireless settings through WPS. For more information, see *WPS Wizard for WiFi Connections* on page 57.

2. (Optional) Clear the **Enable Router's PIN** check box.

The modem router's PIN is disabled. By default, the PIN is enabled, but there might be situations in which you want to disable the PIN.

The PIN function might temporarily be disabled when the modem router detects suspicious attempts to break into the modem router's wireless settings by using the modem router's PIN through WPS. You can manually enable the PIN function by selecting the **Enable Router's PIN** check box.

3. (Optional) Under the Enable Router's PIN check box, type a number in the field.  
By default, the number is 3. This number specifies the number of times that a PIN connection is allowed to fail. You can change this setting only when the PIN is enabled.
4. (Optional) Clear the check box *under* the Enable Router's PIN check box to turn off automatic disabling of the PIN.  
You can change this setting only when the PIN is enabled. By default, automatic disabling of the PIN is turned on.
5. (Optional) Clear the **Keep Existing Wireless Settings** check box.  
By default, the Keep Existing Wireless Settings check box is selected. NETGEAR recommends that you leave this check box selected. However, when the check box is selected, some applications such as Network Explorer in Windows Vista might not detect the modem router.



**CAUTION:**

When you clear the Keep Existing Wireless Settings check box and you add a new wireless client through WPS, the modem router's wireless settings change to an automatically generated SSID and passphrase (also referred to as the wireless network password or network key).

6. Click the **Apply** button.  
Your settings are saved.

## Set Up a Wireless Access List by MAC Address

By default, any wireless device that is configured with the correct SSID is allowed access to your wireless network. For increased security, you can restrict access to the wireless network to allow only specific wireless devices based on their MAC addresses.

Each network device has a MAC address, which is a unique 12-character physical address, containing the hexadecimal characters 0–9, a–f, or A–F (uppercase or lowercase) only, and separated by colons (for example, 00:09:AB:CD:EF:01). Typically, the MAC address is on the label of the wireless card or network interface device. If you do not have access to the label, you can display the MAC address using the network configuration utilities of the computer. You might also find the MAC addresses on the Attached Devices screen.

---

**Note:** If you use a wireless computer to set up a wireless card access list, add your wireless computer to the access list; otherwise, you are disconnected when you click the Apply button. To avoid this situation, use a computer with a wired connection to access the modem router.

---

➤ **To restrict access based on MAC addresses:**

1. Select **ADVANCED > Advanced Setup > Wireless Settings**.
2. Click the **Set Up Access List** button.

3. Click the **Add** button.

4. In the Device Name field, type a name for the wireless device.
5. In the MAC Address field, type the MAC address of the wireless device.

**Tip:** You can also copy and paste the MAC addresses from the Attached Devices screen into the MAC Address field on this screen. To do this, use each wireless computer to join the wireless network. The computer then displays on the Attached Devices screen.

6. Click the **Add** button.

The wireless device is added to the table on the Wireless Card Access List screen.

7. (Optional) Repeat [Step 4](#) through [Step 6](#) for additional wireless devices.
8. Select the **Turn Access Control On** check box.
9. Click the **Apply** button.

Now only wireless devices that are in the table on the Wireless Card Access List screen can access the modem router.

➤ **To change a wireless device on the access list:**

1. Select **ADVANCED > Advanced Setup > Wireless Settings**.

The Advanced Wireless Settings screen displays.

2. In the table, select the radio button next to the wireless device for which you want to make a change.

3. Click the **Edit** button.

The Edit Wireless Card screen displays.

4. Change the settings.
5. Click the **Accept** button.

The changed settings are shown in the table on the Wireless Card Access List screen.

➤ **To delete a wireless device from the access list:**

1. Select **ADVANCED > Advanced Setup > Wireless Settings**.

The Advanced Wireless Settings screen displays.

2. In the table, select the radio button next to the wireless device that you want to remove.
3. Click the **Delete** button.

The address is removed from the table on the Wireless Card Access List screen.

## Wireless Distribution System

You can set the modem router up to be used as a wireless base station or a wireless repeater in a wireless distribution system (WDS). A WDS lets you expand a wireless network through multiple access points. A wireless base station connects to the Internet, can have wired and wireless clients, and sends its wireless signal to an access point that functions as a wireless repeater. A wireless repeater can also have wired and wireless clients, but connects to the Internet through the wireless base station. The following figure shows a wireless repeating scenario.

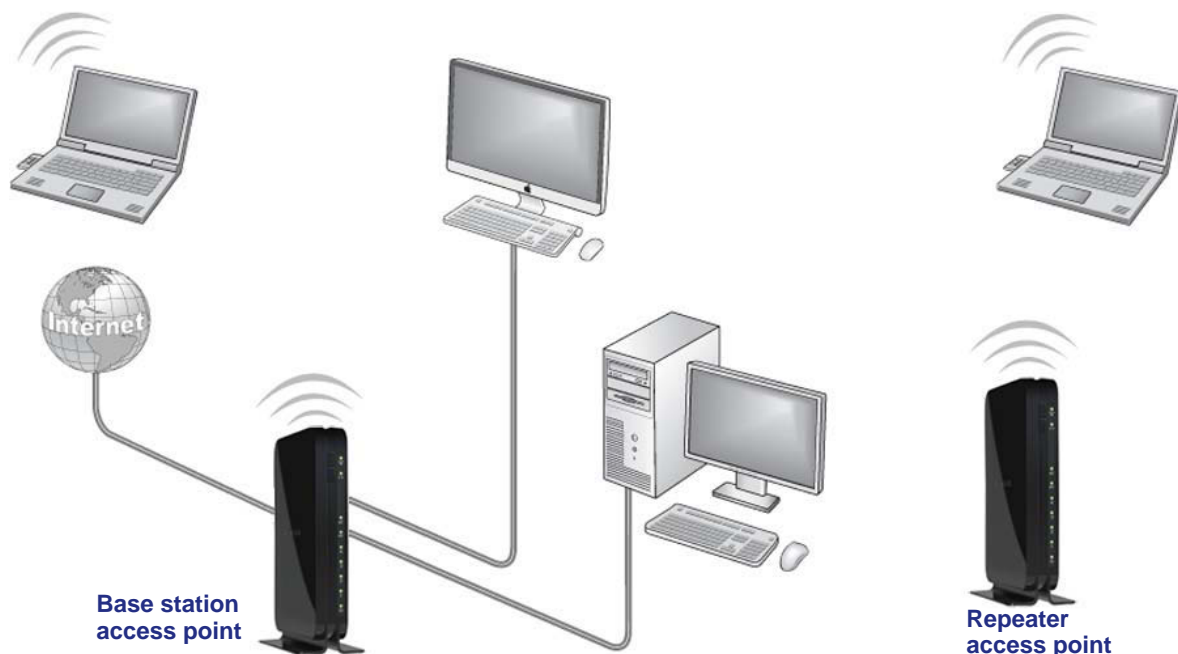


Figure 17. Wireless repeating scenario



The modem router can function either as a base station or as a repeater:

- **Wireless base station.** The modem router acts as the parent access point, bridging traffic to and from the child repeater access point, as well as handling wireless and wired local computers. To configure this mode, you must know the MAC address of the child repeater access point.
- **Wireless repeater.** The modem router sends all traffic from its local wireless or wired computers to a remote access point. To configure this mode, you must know the MAC address of the remote parent access point.

For you to set up a wireless network in a WDS, the following conditions must be met for both access points:

- Both access points must use the same SSID, wireless channel, and encryption mode.
- Both access points must be on the same LAN IP subnet. That is, all the access point LAN IP addresses are in the same network.
- All LAN devices (wired and wireless computers) must be configured to operate in the same LAN network address range as the access points.
- The channel selection on the access points cannot be Auto (see *Basic Wireless Settings* on page 36).
- The security option needs to be WEP (see *Basic Wireless Settings* on page 36).

---

**Note:** When you use the wireless repeating function, WPS becomes disabled.

---

## Set Up the Base Station

The wireless repeating function works only in hub and spoke mode. The units cannot be daisy-chained. You must know the wireless MAC addresses of all units. First, set up the base station, and then set up the repeater.

➤ **To set up the base station:**

1. Select **ADVANCED > Advanced Setup > Wireless Repeating Function**.

The Wireless Repeating Function screen displays. The wireless MAC address of the modem router is displayed onscreen.

2. Select the **Enable Wireless Repeating Function** check box.



3. Select the **Wireless Base Station** radio button.

4. (Optional) Select the **Disable Wireless Client Association** check box.

Wireless clients are prevented from associating with the base station and LAN client associations only are allowed. You can leave the check box cleared if you prefer wireless clients to be able to associate with the base stations.

5. In the Repeater MAC Address 1 through 4 fields, enter the MAC addresses for the access points that you want to function as repeaters.

If your modem router is the base station, it can function as the “parent” for up to four other access points.

6. Click the **Apply** button.

Your settings are saved.

## Set Up a Repeater

Use a wired Ethernet connection to set up the repeater to avoid conflicts with the wireless connection to the base station.

---

**Note:** If you set up the modem router as a base station with a non-NETGEAR access point as the repeater, you might need to change additional configuration settings. In particular, you should disable the DHCP server function on the access point that functions as the repeater.

---

➤ **To configure the modem router as a repeater:**

1. Select **ADVANCED > Advanced Setup > Wireless Repeating Function**.

The Wireless Repeating Function screen displays. The wireless MAC address of the modem router is displayed onscreen.

2. Select the **Enable Wireless Repeating Function** check box.
3. Select the **Wireless Repeater** radio button.

4. Fill in the Repeater IP Address fields.

This IP address needs to be in the same subnet as the base station, but different from the LAN IP address of the base station.

5. (Optional) Select the **Disable Wireless Client Association** check box.

Wireless clients are prevented from associating with the repeater and LAN client associations only are allowed. You can leave the check box cleared if you prefer wireless clients to be able to associate with the repeater.

6. In the Base Station MAC Address field, enter the MAC addresses for the access point that you want to function as the base station.

7. Click the **Apply** button.

Your settings are saved.

8. Verify connectivity across the LANs:

- Verify that a computer on any wireless or wired LAN segment of the base station or a repeater can connect to the Internet.
- Verify that any computer that is connected to the base station can share files and printers with any other wireless or wired computer or server that is connected to a repeater, and the other way around.

## Port Forwarding and Port Triggering

By default, the modem router blocks inbound traffic from the Internet to your computers except replies to your outbound traffic. You might need to create exceptions to this rule for these purposes:

- To enable remote computers on the Internet to access a server on your local network.
- To enable certain applications and games to work correctly if the modem router does not recognize their replies.

Your modem router provides two features for creating these exceptions: port forwarding and port triggering. The next sections provide background information to help you understand how port forwarding and port triggering work, and the differences between the two.

### Remote Computer Access Basics

When a computer on your network needs to access a computer on the Internet, your computer sends your modem router a message containing the source and destination address and process information. Before forwarding your message to the remote computer, your modem router has to modify the source information and create and track the communication session so that replies can be routed back to your computer.

Here is an example of normal outbound traffic and the resulting inbound responses:

1. You open a browser, and your operating system assigns port number 5678 to this browser session.
2. You type `http://www.example.com` into the URL field, and your computer creates a web page request message with the following address and port information. The request message is sent to your modem router:
  - **Source address.** Your computer's IP address
  - **Source port number.** 5678, which is the browser session
  - **Destination address.** The IP address of `www.example.com`, which your computer finds by asking a DNS server
  - **Destination port number.** 80, which is the standard port number for a web server process
3. Your modem router creates an entry in its internal session table describing this communication session between your computer and the web server at `www.example.com`. Before sending the web page request message to `www.example.com`, your modem router stores the original information and then modifies the source information in the request message, performing Network Address Translation (NAT):
  - The source address is replaced with your modem router's public IP address. This requirement is necessary because your computer uses a private IP address that is not globally unique and cannot be used on the Internet.
  - The source port number is changed to a number chosen by the modem router, such as 33333. This requirement is necessary because two computers might independently be using the same session number.

Your modem router then sends this request message through the Internet to the web server at [www.example.com](http://www.example.com).

4. The web server at [www.example.com](http://www.example.com) composes a return message with the requested web page data. The return message contains the following address and port information. The web server then sends this reply message to your modem router:
  - **Source address.** The IP address of [www.example.com](http://www.example.com)
  - **Source port number.** 80, which is the standard port number for a web server process
  - **Destination address.** The public IP address of your modem router
  - **Destination port number.** 33333
5. Upon receiving the incoming message, your modem router checks its session table to determine whether there is an active session for port number 33333. Finding an active session, the modem router then modifies the message to restore the original address information replaced by NAT. Your modem router sends this reply message to your computer, which displays the web page from [www.example.com](http://www.example.com). The message now contains the following address and port information:
  - **Source address.** The IP address of [www.example.com](http://www.example.com)
  - **Source port number.** 80, which is the standard port number for a web server process
  - **Destination address.** Your computer's IP address
  - **Destination port number.** 5678, which is the browser session that made the initial request
6. When you finish your browser session, your modem router eventually detects a period of inactivity in the communications. Your modem router then removes the session information from its session table, and incoming traffic is no longer accepted on port number 33333.

## Port Triggering to Open Incoming Ports

Some application servers (such as FTP and IRC servers) send replies to multiple port numbers. Using the port triggering function of your modem router, you can tell the modem router to open more incoming ports when a particular outgoing port originates a session.

An example is Internet Relay Chat (IRC). Your computer connects to an IRC server at destination port 6667. The IRC server not only responds to your originating source port, but also sends an "identify" message to your computer on port 113. Using port triggering, you can tell the modem router, "When you initiate a session with destination port 6667, you must also allow incoming traffic on port 113 to reach the originating computer." Using steps similar to the preceding example, the following sequence shows the effects of the port triggering rule you have defined:

1. You open an IRC client program to start a chat session on your computer.
2. Your IRC client composes a request message to an IRC server using a destination port number of 6667, the standard port number for an IRC server process. Your computer then sends this request message to your modem router.
3. Your modem router creates an entry in its internal session table describing this communication session between your computer and the IRC server. Your modem router

stores the original information, performs Network Address Translation (NAT) on the source address and port, and sends this request message through the Internet to the IRC server.

4. Noting your port triggering rule and having observed the destination port number of 6667, your modem router creates an additional session entry to send any incoming port 113 traffic to your computer.
5. The IRC server sends a return message to your modem router using the NAT-assigned source port (for example, port 33333) as the destination port. The IRC server also sends an “identify” message to your modem router with destination port 113.
6. Upon receiving the incoming message to destination port 33333, your modem router checks its session table to determine whether there is an active session for port number 33333. Finding an active session, the modem router restores the original address information replaced by NAT and sends this reply message to your computer.
7. Upon receiving the incoming message to destination port 113, your modem router checks its session table and learns that there is an active session for port 113 associated with your computer. The modem router replaces the message’s destination IP address with your computer’s IP address and forwards the message to your computer.
8. When you finish your chat session, your modem router eventually senses a period of inactivity in the communications. The modem router then removes the session information from its session table, and incoming traffic is no longer accepted on port numbers 33333 or 113.

To configure port triggering, you must know which inbound ports the application needs. Also, you must know the number of the outbound port that will trigger the opening of the inbound ports. You can usually determine this information by contacting the publisher of the application or the user groups or news groups.

---

**Note:** Only one computer at a time can use the triggered application.

---

## Port Forwarding to Permit External Host Communications

In both of the preceding examples, your computer initiates an application session with a server computer on the Internet. However, you might need to allow a client computer on the Internet to initiate a connection to a server computer on your network. Normally, your modem router ignores any inbound traffic that is not a response to your own outbound traffic. You can configure exceptions to this default rule by using the port forwarding feature.

A typical application of port forwarding can be shown by reversing the client-server relationship from the previous web server example. In this case, a remote computer’s browser needs to access a web server running on a computer in your local network. Using port forwarding, you can tell the modem router, “When you receive incoming traffic on port 80 (the standard port number for a web server process), forward it to the local computer at 192.168.0.123.”

The following sequence shows the effects of the port forwarding rule you have defined:

1. The user of a remote computer opens a browser and requests a web page from `www.example.com`, which resolves to the public IP address of your modem router. The remote computer composes a web page request message with the following destination information:
  - **Destination address.** The IP address of `www.example.com`, which is the address of your modem router
  - **Destination port number.** 80, which is the standard port number for a web server process

The remote computer then sends this request message through the Internet to your modem router.

2. Your modem router receives the request message and looks in its rules table for any rules covering the disposition of incoming port 80 traffic. Your port forwarding rule specifies that incoming port 80 traffic needs to be forwarded to local IP address `192.168.0.123`. Therefore, your modem router modifies the destination information in the request message:

The destination address is replaced with `192.168.0.123`.

Your modem router then sends this request message to your local network.

3. Your web server at `192.168.0.123` receives the request and composes a return message with the requested web page data. Your web server then sends this reply message to your modem router.
4. Your modem router performs Network Address Translation (NAT) on the source IP address, and sends this request message through the Internet to the remote computer, which displays the web page from `www.example.com`.

To configure port forwarding, you must know which inbound ports the application needs. You usually can determine this information by contacting the publisher of the application or the relevant user groups or news groups.

## How Port Forwarding Differs from Port Triggering

The following points summarize the differences between port forwarding and port triggering:

- Any computer on your network can use port triggering, although only one computer can use it at a time.
- Port forwarding is configured for a single computer on your network.
- With port triggering, the modem router does not need to know the computer's IP address in advance. The IP address is captured automatically.
- Port forwarding requires that you specify the computer's IP address during configuration, and the IP address can never change.
- Port triggering requires specific outbound traffic to open the inbound ports, and the triggered ports are closed after a period of no activity.
- Port forwarding is always active and does not need to be triggered.



## Set Up Port Forwarding to Local Servers

The port forwarding feature lets you allow certain types of incoming traffic to reach servers on your local network. For example, you might want to make a local web server, FTP server, or game server visible and available to the Internet.

Use the Port Forwarding / Port Triggering screen to configure the modem router to forward specific incoming protocols to computers on your local network. In addition to servers for specific applications, you can also specify a default DMZ server to which all other incoming protocols are forwarded.

Before you start, determine which type of service, application, or game you want to provide, and the local IP address of the computer that will provide the service. The server computer needs to always have the same IP address.

To ensure that your server computer always has the same IP address, use the reserved IP address feature of your product. For more information, see [Set Up Address Reservation](#) on page 56.

### ➤ To forward specific incoming protocols:

1. Select **ADVANCED > Advanced Setup > Port Forwarding/Port Triggering**.

Port Forwarding / Port Triggering

Please select the service type.

Port Forwarding  
 Port Triggering

Service Name: FTP(TCP:20,21) Server IP Address: [ ] [ ] [ ] [ ] + Add

#	Service Name	External Start Port	External End Port	Internal Start Port	Internal End Port	Internal IP address
---	--------------	---------------------	-------------------	---------------------	-------------------	---------------------

Edit Service Delete Service

+ Add Custom Service

2. Leave the Port Forwarding radio button selected as the service type.
3. From the Service Name menu, select the service or game that you plan to host on your network.

If the service does not display in the menu, see [Manage Custom Services for Port Forwarding](#) on page 112.

4. In the Server IP Address fields, type the IP address of your local computer that needs to receive the inbound traffic that is covered by this inbound firewall rule.
5. Click the **Add** button.

The service is added to the table on the Port Forwarding / Port Triggering screen.

## Manage Custom Services for Port Forwarding

Before you define a service, game, or application that does not display in the Service Name menu on the Port Forwarding / Port Triggering screen, first determine which port number or range of numbers the application uses. You can usually determine this information by contacting the publisher of the application or user groups or news groups. When you have the port number information, follow these steps.

➤ **To add a custom service for port forwarding:**

1. Select **ADVANCED > Advanced Setup > Port Forwarding/Port Triggering**.

The Port Forwarding / Port Triggering screen displays.

2. Select the **Port Forwarding** radio button as the service type.
3. Click the **Add Custom Service** button.

Or select from currently attached devices		
	IP Address	Device Name
<input type="radio"/>	192.168.0.200	VOSTRO1500

4. In the Service Name field, enter a descriptive name.
5. From the Protocol menu, select the correct type of protocol for the new service:
  - TCP
  - UDP
  - TCP/UDP

**Note:** *If you are not sure which protocol to select, select **TCP/UDP**.*

6. In the External Starting Port field, enter the starting port number for the new service or application.
7. In the External Ending Port field, enter the ending port number for the new service or application.

If the service or application uses a single port number, enter that number in both fields.



8. Specify the internal ports by one of these methods:
  - Leave the **Use the same port range for Internal port** check box selected.
  - Fill in the Internal Starting Port.

**Note:** *The Internal Ending Port field is masked out because the ending port number is calculated automatically by using the same range as the external port range.*

9. Specify the internal IP address by one of these methods:
  - In the Internal IP Address fields, type the internal IP address.
  - Select the radio button for an attached device that is listed in the table.

10. Click the **Apply** button.

The custom service is added to the table on the Port Forwarding / Port Triggering screen.

➤ **To change a port forwarding entry in the table on the Port Forwarding / Port Triggering screen:**

1. Select **ADVANCED > Advanced Setup > Port Forwarding/Port Triggering**.

The Port Forwarding / Port Triggering screen displays.

2. Select the **Port Forwarding** radio button as the service type.
3. In the table, select the radio button next to the service that you want to change.
4. Click the **Edit Service** button.

The Ports - Custom Services screen displays.

5. Change the settings for the service.
6. Click the **Apply** button.

The changed settings of the service are shown in table on the Port Forwarding / Port Triggering screen.

➤ **To remove a port forwarding entry from the table on the Port Forwarding / Port Triggering screen:**

1. Select **ADVANCED > Advanced Setup > Port Forwarding/Port Triggering**.

The Port Forwarding / Port Triggering screen displays.

2. Select the **Port Forwarding** radio button as the service type.
3. In the table, select the radio button to the left of the service that you want to remove.
4. Click the **Delete Service** button.

The service is removed from the table on the Port Forwarding / Port Triggering screen.

## Application Example: Make a Local Web Server Public

If you host a web server on your local network, you can use port forwarding to allow web requests from anyone on the Internet to reach your web server.

➤ **To make a local web server public:**

1. Assign your web server either a fixed IP address or a dynamic IP address using DHCP address reservation.

In this example, your modem router always gives your web server an IP address of 192.168.0.33.

2. On the Port Forwarding / Port Triggering screen, configure the modem router to forward the HTTP service to the local address of your web server at **192.168.0.33**.

HTTP (port 80) is the standard protocol for web servers.

3. (Optional) Register a host name with a Dynamic DNS service, and configure your modem router to use the name.

To access your web server from the Internet, a remote user has to know the IP address that your ISP assigned. However, if you use a Dynamic DNS service, the remote user can reach your server by a user-friendly Internet name, such as mynetgear.dyndns.org.

## Set Up and Manage Port Triggering

Port triggering is a dynamic extension of port forwarding that is useful in these cases:

- More than one local computer needs port forwarding for the same application (but not simultaneously).
- An application needs to open incoming ports that are different from the outgoing port.

When port triggering is enabled, the modem router monitors outbound traffic looking for a specified outbound “trigger” port. When the modem router detects outbound traffic on that port, it remembers the IP address of the local computer that sent the data. The modem router then temporarily opens the specified incoming port or ports and forwards incoming traffic on the triggered ports to the triggering computer.

Port forwarding creates a static mapping of a port number or range to a single local computer. Port triggering can dynamically open ports to any computer that needs them and can close the ports when they are no longer needed.

---

**Note:** If you use applications such as multiplayer gaming, peer-to-peer connections, real-time communications such as instant messaging, or remote assistance (a feature in Windows XP), NETGEAR recommends that you also enable Universal Plug and Play (UPnP). For more information, see *Universal Plug and Play* on page 122.

---

## Manage Port Triggering

By default, port triggering is enabled with a time-out period of 20 minutes.

The time-out value controls the inactivity timer for the designated inbound ports. The inbound ports close when the inactivity time expires. This is required because the modem router cannot detect when the application has terminated.

If you disable port triggering after you configured port triggering services, the services are retained even though they are not used.

➤ **To change the port triggering time-out period:**

1. Select **ADVANCED > Advanced Setup > Port Forwarding/Port Triggering**.
2. Select the **Port Triggering** radio button.

3. In the Port Triggering Time-out field, enter a value up to 9999 minutes.  
By default, the port triggering time-out is 20 minutes.

4. Click the **Apply** button.  
Your settings are saved.

➤ **To disable port triggering:**

1. Select **ADVANCED > Advanced Setup > Port Forwarding/Port Triggering**.  
The Port Forwarding / Port Triggering screen displays.
2. Select the **Port Triggering** radio button.
3. Select the **Disable Port Triggering** check box.
4. Click the **Apply** button.  
Your settings are saved.

## Manage Port Triggering Services

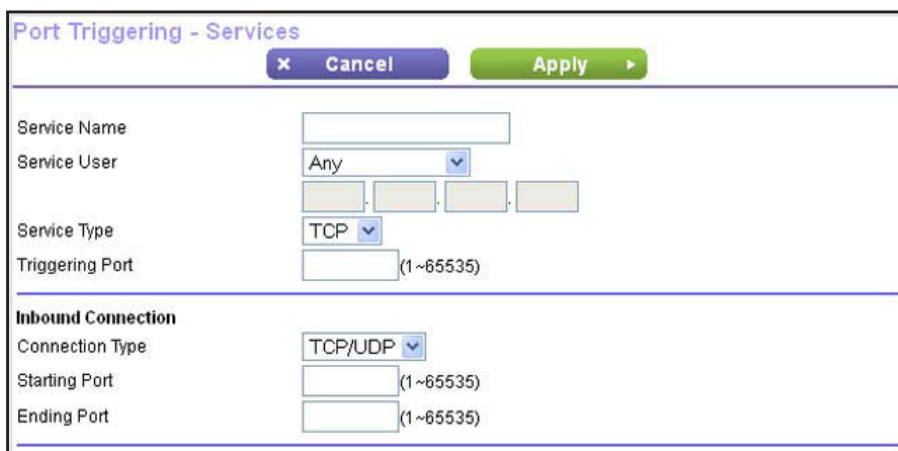
To configure port triggering services, you must know which inbound ports the application needs, and the number of the outbound port that will trigger the opening of the inbound ports. You can usually determine this information by contacting the publisher of the application or user groups or news groups.

➤ **To add a port triggering service:**

1. Select **ADVANCED > Advanced Setup > Port Forwarding/Port Triggering**.

The Port Forwarding / Port Triggering screen displays.

2. Select the **Port Triggering** radio button.
3. Click the **Add Service** button.



4. In the Service Name field, type a descriptive service name.
5. Select how the service affects users:
  - a. Selection an option from the Service User menu:
    - **Any**. Lets any computer on the Internet use this service. This is the default selection.
    - **Single address**. Restricts the service to a particular computer.
  - b. If you select Single address, type the IP address in the fields.
6. From the Service Type menu, select the correct type of protocol for the new service:
  - **TCP**
  - **UDP**
7. In the Triggering Port field, enter the number of the outbound traffic port that will cause the inbound ports (see [Step 9](#) and [Step 10](#)) to be opened.
8. From the Connection Type menu, select the correct type of protocol for the inbound connection:
  - **TCP/UDP**
  - **TCP**
  - **UDP**

**Note:** *If you are not sure which protocol to select, select **TCP/UDP**.*

9. In the Starting Port field, enter the starting port number for the inbound connection.
10. In the Ending Port field, enter the ending port number for the inbound connection.  
If the inbound connection uses a single port number, enter that number in both fields.
11. Click the **Apply** button.

The new service is added to the Port Triggering Portmap Table on the Port Forwarding / Port Triggering screen.

➤ **To disable an existing port triggering service:**

1. Select **ADVANCED > Advanced Setup > Port Forwarding/Port Triggering**.  
The Port Forwarding / Port Triggering screen displays.
2. Select the **Port Triggering** radio button.
3. In the Port Triggering Portmap Table, clear the **Enable** check box for the service that you want to disable.
4. Click the **Apply** button.  
Your settings are saved.

➤ **To change an existing port triggering service:**

1. Select **ADVANCED > Advanced Setup > Port Forwarding/Port Triggering**.  
The Port Forwarding / Port Triggering screen displays.
2. Select the **Port Triggering** radio button.
3. In the Port Triggering Portmap Table, select the radio button next to the service that you want to change.
4. Click the **Edit Service** button.  
The Port Triggering - Services screen displays.
5. Change the settings for the service.
6. Click the **Apply** button.

The changed settings of the service are shown in the Port Triggering Portmap Table on the Port Forwarding / Port Triggering screen.

➤ **To remove an existing port triggering service:**

1. Select **ADVANCED > Advanced Setup > Port Forwarding/Port Triggering**.  
The Port Forwarding / Port Triggering screen displays.
2. Select the **Port Triggering** radio button.
3. In the Port Triggering Portmap Table, select the radio button to the left of the service that you want to remove.
4. Click the **Delete Service** button.

The service is removed from the Port Triggering Portmap Table on the Port Forwarding / Port Triggering screen.

## Dynamic DNS

If your Internet service provider (ISP) gave you a permanently assigned (fixed) IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you do not know your IP address in advance, and the address can change frequently. In this case, you can use a commercial Dynamic DNS service. This type of service lets you register your domain to their IP address and forwards traffic directed at your domain to your frequently changing IP address.

If your ISP assigns a private WAN IP address (such as 192.168.x.x or 10.x.x.x), the Dynamic DNS service does not work because private addresses are not routed on the Internet.

Your modem router contains a client that can connect to the Dynamic DNS service provided by DynDNS.org. First visit their website at <http://www.dyndns.org> and obtain an account and host name that you configure in the modem router. Then, whenever your ISP-assigned IP address changes, your modem router automatically contacts the Dynamic DNS service provider, logs in to your account, and registers your new IP address. If your host name is hostname, for example, you can reach your modem router at <http://hostname.dyndns.org>.

### ➤ To set up Dynamic DNS:

1. Register for an account with one of the Dynamic DNS service providers whose URLs are in the Service Provider menu.
2. Select **ADVANCED > Advanced Setup > Dynamic DNS**.

3. Select the **Use a Dynamic DNS Service** check box.
4. Select the URL of your Dynamic DNS service provider.  
For example, for DynDNS.org, select **www.DynDNS.org**. The DNS service providers that you can select from the menu depend on the region and country in which you use the modem router.
5. In the Host name field, type the host or domain name that your Dynamic DNS service provider gave you.
6. In the User Name field, type the user name for your Dynamic DNS account.

This is the name that you use to log in to your account, not your host name.

7. In the Password field, type the password or key for your Dynamic DNS account.
8. Click the **Apply** button.

Your settings are saved.

## Static Routes

Static routes provide more routing information to your modem router. Typically, you do not need to add static routes. You need to configure static routes only for unusual cases such as multiple modem routers or multiple IP subnets on your network.

As an example of when a static route is needed, consider the following case:

- Your primary Internet access is through a cable modem to an ISP.
- You have an ISDN router on your home network for connecting to the company where you are employed. This router's address on your LAN is 192.168.0.100.
- Your company's network address is 134.177.0.0.

When you first configured your modem router, two implicit static routes were created. A default route was created with your ISP as the gateway, and a second static route was created to your local network for all 192.168.0.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your modem router forwards your request to the ISP. The ISP forwards your request to the company where you are employed, and the request is likely to be denied by the company's firewall.

In this case you need to define a static route, instructing your modem router that 134.177.0.0 is accessed through the ISDN modem router at 192.168.0.100. In this example:

- The Destination IP Address and IP Subnet Mask fields specify that this static route applies to all 134.177.x.x addresses.
- The Gateway IP Address field specifies that all traffic for these addresses is forwarded to the ISDN modem router at 192.168.0.100.
- A metric value of 1 works because the ISDN modem router is on the LAN.
- Private is selected only as a precautionary security measure in case RIP is activated.

### ➤ To set up a static route:

1. Select **ADVANCED > Advanced Setup > Static Routes**.



- Click the **Add** button.



- In the Route Name field, type a name for this static route.  
This name is for identification purposes only.
- (Optional) To limit access to the LAN only, select the **Private** check box.  
If Private is selected, the static route is not reported in RIP.
- (Optional) To prevent the route from becoming effective after you click the Apply button, clear the **Active** check box.  
By default, the Active check box is selected and a route becomes effective after you click the Apply button.
- In the Destination IP Address fields, type the IP address of the final destination of the route.
- In the IP Subnet Mask fields, type the IP subnet mask of the final destination of the route.  
If the destination is a single host, type **255.255.255.255**.
- In the Gateway IP Address fields, type the IP address of the gateway, which needs to be on the same LAN segment as the modem router.
- In the Metric field, type a number from 1 through 15 as the metric value.  
This value represents the number of modem routers between your network and the destination. Usually, a setting of 2 or 3 works, but if this is a direct connection, set it to 1.
- Click the **Apply** button.  
The static route is added to the table on the Static Route screen.

➤ **To change a static route:**

- Select **ADVANCED > Advanced Setup > Static Routes**.  
The Static Routes screen displays.
- In the table, select the radio button next to the route that you want to change.
- Click the **Edit** button.
- Change the settings for the route.
- Click the **Apply** button.  
The changed settings of the route are shown in the table on the Static Routes screen.



➤ **To remove a static route:**

1. Select **ADVANCED > Advanced Setup > Static Routes**.

The Static Routes screen displays.

2. In the table, select the radio button to the left of the route that you want to remove.
3. Click the **Delete** button.

The route is removed from the table on the Static Routes screen.

## Remote Management

The remote management feature lets you update or check the status of your modem router over the Internet.

---

**Note:** Be sure to change the modem router default login password to a secure password. A secure password contains no dictionary words from any language and contains uppercase and lowercase letters, numbers, and symbols. It can be up to 30 characters. For more information, see *Change the Password* on page 91.

---

For enhanced security, restrict access to as few external IP addresses as practical.

➤ **To set up remote management:**

1. Select **ADVANCED > Advanced Setup > Remote Management**.

2. Select the **Turn Remote Management On** check box.
3. Specify the external IP address or addresses from which the modem router can be managed remotely:
  - For a single IP address on the Internet:
    - a. Select the **Only This Computer** radio button.
    - b. Enter the IP address from which access is allowed.

- For a range of IP addresses on the Internet:
  - a. Select **IP Address Range** radio button.
  - b. In the From fields, enter the start IP address of the range from which access is allowed.
  - c. In the To fields, enter the end IP address of the range from which access is allowed.
- For all IP addresses on the Internet, keep the **Everyone** radio button selected.  
This is the default setting.

4. Specify the port number for accessing the web management interface.

Normal web browser access uses the standard HTTP service port 80. For greater security, enter a custom port number for the remote web management interface. Choose a number from 1024 to 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.

5. Click the **Apply** button.

Your changes take effect.

When you access your modem router from the Internet, type your modem router's WAN IP address in your browser's address or location field followed by a colon (:) and the custom port number. For example, if your external address is 203.0.113.123 and you use port number 8080, enter **http://203.0.113.123:8080** in your browser.

## Universal Plug and Play

Universal Plug and Play (UPnP) helps devices, such as Internet appliances and computers, access the network and connect to other devices as needed. UPnP devices can automatically discover the services from other registered UPnP devices on the network.

If you use applications such as multiplayer gaming, peer-to-peer connections, or real-time communications such as instant messaging or remote assistance, NETGEAR recommends that you enable UPnP.

➤ **To turn on Universal Plug and Play:**

1. Select **ADVANCED > Advanced Setup > UPnP**.

Active	Protocol	Int. Port	Ext. Port	IP Address

2. Select the **Turn UPnP On** check box.

By default, this check box is selected. You can disable UPnP for automatic device configuration. If you clear the Turn UPnP On check box, the modem router does not allow any device to automatically control the resources, such as port forwarding (mapping), of the modem router.

3. Type the advertisement period in minutes.

The advertisement period specifies how often the modem router broadcasts its UPnP information. This value can range from 1 to 1440 minutes. The default period is 30 minutes. Shorter durations ensure that control points have current device status at the expense of additional network traffic. Longer durations can compromise the freshness of the device status, but can significantly reduce network traffic.

4. Type the advertisement time to live in hops.

The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. Hops are the steps a packet takes between routers. The number of hops can range from 1 to 255. The default value for the advertisement time to live is 4 hops, which is fine for most home networks. If you notice that some devices are not being updated or reached correctly, it might be necessary to increase this value.

5. Click the **Apply** button.

The UPnP Portmap Table displays the IP address of each UPnP device that is accessing the modem router and which internal and external port that device has opened. The UPnP Portmap table also displays what type of port is open and whether that port is still active for each IP address.

6. (Optional) To refresh the information in the UPnP Portmap Table, click the **Refresh** button.

## IPv6

You can use this feature to set up an IPv6 Internet connection type if genie does not detect it automatically.

- **To set up an IPv6 Internet connection type:**

1. Select **ADVANCED > Advanced Setup > IPv6**.



2. Select the IPv6 connection type from the menu.

Your Internet service provider (ISP) can provide information about your IPv6 connection.

- If your ISP did not provide details, you can select **6to4 Tunnel**.
- If you are not sure what type of IPv6 connection the modem router uses, select **Auto Detect** so that the modem router detects the IPv6 type that is in use.
- If your Internet connection does not use PPPoE, DHCP, a fixed IP address, or pass-through but is IPv6, select **Auto Config**.

---

**Note:** For IPv6 address requirements, information about IPv6 filtering, and detailed information about IPv6 Internet connection types, see the following sections.

---

3. Click the **Apply** button.

Your settings are saved.

## Requirements for Entering IPv6 Addresses

IPv6 addresses are denoted by eight groups of hexadecimal quartets that are separated by colons. Any four-digit group of zeroes within an IPv6 address can be reduced to a single zero or altogether omitted.

The following errors invalidate an IPv6 address:

- More than eight groups of hexadecimal quartets
- More than four hexadecimal characters in a quartet
- More than two colons in a row

## IPv6 Filtering

When you enable IPv6 and select any connection type other than IPv6 Pass Through, the modem router starts the stateful packet inspection (SPI) firewall function on the WAN interface. The modem router creates connection records and checks every inbound IPv6 packet. If the inbound packet is not destined to the modem router itself and the modem router does not expect to receive such a packet, or the packet is not in the connection record, the modem router blocks this packet. This function has two modes:

- **Secured.** In secured mode, the modem router inspects both TCP and UDP packets.
- **Open.** In open mode, the modem router inspects UDP packets only.

## Auto Detect

- **To set up an IPv6 Internet connection through auto detection:**
1. Select **ADVANCED > Advanced Setup > IPv6**.
  2. From the Internet Connection Type menu, select **Auto Detect**.

The screen adjusts:

The screenshot shows the IPv6 configuration page. At the top, there are three buttons: 'Status Refresh', 'Cancel', and 'Apply'. Below the buttons, the 'Internet Connection Type' is set to 'Auto Detect'. The 'Connection Type' is 'the Internet port is not connected'. The 'Router's IPv6 Address On WAN' is 'Not Available'. The 'LAN Setup' section shows 'Router's IPv6 Address On LAN1' as 'Not Available'. Under 'IP Address Assignment', 'Auto Config' is selected with a radio button. There is an unchecked checkbox for 'Use This Interface ID' with four empty input boxes below it. At the bottom, 'IPv6 Filtering' is set to 'Secured'.

The modem router automatically detects the information in the following fields:

- **Connection Type.** This field indicates the connection type that is detected.
  - **Router's IPv6 Address on WAN.** This field shows the IPv6 address that is acquired for the modem router's WAN (or Internet) interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline ( ) under the IPv6 address. If no address is acquired, the field displays Not Available.
  - **Router's IPv6 Address on LAN1.** This field shows the IPv6 address that is acquired for the modem router's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline ( ) under the IPv6 address. If no address is acquired, the field displays Not Available.
3. Specify how the modem router assigns IPv6 addresses to the devices on your home network (the LAN) by selecting one of the following radio buttons:
    - **Use DHCP Server.** This method passes more information to LAN devices, but some IPv6 systems might not support the DHCv6 client function.
    - **Auto Config.** This is the default setting.
  4. (Optional) Select the **Use This Interface ID** check box, and specify the interface ID that you want to be used for the IPv6 address of the modem router's LAN interface.

If you do not specify an ID here, the modem router generates one automatically from its MAC address.

5. Specify the IPv6 filtering mode by selecting one of the following radio buttons:
  - **Secured.** In the secured mode, which is the default mode, the modem router inspects both TCP and UDP packets.
  - **Open.** In the open mode, the modem router inspects UDP packets only.
6. Click the **Apply** button.  
Your settings are saved.

## IPv6 Auto Config

- To set up an IPv6 Internet connection through auto configuration:
  1. Select **ADVANCED > Advanced Setup > IPv6**.
  2. From the Internet Connection Type menu, select **Auto Config**.

The screen adjusts:

The modem router automatically detects the information in the following fields:

- **Router's IPv6 Address on WAN.** This field shows the IPv6 address that is acquired for the modem router's WAN (or Internet) interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (\_\_) under the IPv6 address. If no address is acquired, the field displays Not Available.
- **Router's IPv6 Address on LAN1.** This field shows the IPv6 address that is acquired for the modem router's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (\_\_) under the IPv6 address. If no address is acquired, the field displays Not Available.

3. (Optional) In the DHCP User Class (If Required) field, enter a host name.  
If your ISP has given you a specific host name, enter it here. Otherwise, leave this field blank.
4. (Optional) In the DHCP Domain Name (If Required) field, enter a domain name.  
You can type the domain name of your IPv6 ISP. (Do not enter the domain name for the IPv4 ISP here.) For example, if your ISP's mail server is mail.xxx.yyy.zzz, type xxx.yyy.zzz as the domain name.  
  
If your ISP provided a specific domain name, type it in this field. (For example, Earthlink Cable might require a host name of home, and Comcast sometimes supplies a domain name.)
5. Specify how the modem router assigns IPv6 addresses to the devices on your home network (the LAN) by selecting one of the following radio buttons:
  - **Use DHCP Server.** This method passes more information to LAN devices, but some IPv6 systems might not support the DHCv6 client function.
  - **Auto Config.** This is the default setting.
6. (Optional) Select the **Use This Interface ID** check box, and specify the interface ID that you want to be used for the IPv6 address of the modem router's LAN interface.  
  
If you do not specify an ID here, the modem router generates one automatically from its MAC address.
7. Specify the IPv6 filtering mode by selecting one of the following radio buttons:
  - **Secured.** In the secured mode, which is the default mode, the modem router inspects both TCP and UDP packets.
  - **Open.** In the open mode, the modem router inspects UDP packets only.
8. Click the **Apply** button.  
  
Your settings are saved.

## IPv6 6to4 Tunnel

The remote relay router is the router to which your modem router creates the 6to4 tunnel. Make sure that the IPv4 Internet connection is working before you apply the 6to4 tunnel settings for the IPv6 connection.

- **To set up an IPv6 Internet connection by using a 6to4 tunnel:**
1. Select **ADVANCED > Advanced Setup > IPv6**.
  2. From the Internet Connection Type menu, select **6to4 Tunnel**.

The screen adjusts:

The modem router automatically detects the information in the following field:

- **Router's IPv6 Address on LAN1.** This field shows the IPv6 address that is acquired for the modem router's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (\_\_) under the IPv6 address. If no address is acquired, the field displays Not Available.
3. Configure the remote 6to4 relay router settings by selecting one of the following radio buttons:
    - **Auto.** Your modem router uses any remote relay router that is available on the Internet. This is the default setting.
    - **Static IP Address.** Enter the static IPv4 address of the remote relay router. Your IPv6 ISP usually provides this address.
  4. Specify how the modem router assigns IPv6 addresses to the devices on your home network (the LAN) by selecting one of the following radio buttons:
    - **Use DHCP Server.** This method passes more information to LAN devices, but some IPv6 systems might not support the DHCv6 client function.
    - **Auto Config.** This is the default setting.
  5. (Optional) Select the **Use This Interface ID** check box, and specify the interface ID that you want to be used for the IPv6 address of the modem router's LAN interface.

If you do not specify an ID here, the modem router generates one automatically from its MAC address.



6. Specify the IPv6 filtering mode by selecting one of the following radio buttons:
  - **Secured.** In the secured mode, which is the default mode, the modem router inspects both TCP and UDP packets.
  - **Open.** In the open mode, the modem router inspects UDP packets only.
7. Click the **Apply** button.

Your settings are saved.

## IPv6 Pass Through

In pass-through mode, the modem router works as a Layer 2 Ethernet switch with two ports (LAN and WAN Ethernet ports) for IPv6 packets. The modem router does not process any IPv6 header packets.

- **To set up a pass-through IPv6 Internet connection:**
  1. Select **ADVANCED > Advanced Setup > IPv6**.
  2. From the Internet Connection Type menu, select **Pass Through**.

The screen adjusts, but no additional fields display.
  3. Click the **Apply** button.

Your settings are saved.

## IPv6 Fixed

- **To set up a fixed IPv6 Internet connection:**
  1. Select **ADVANCED > Advanced Setup > IPv6**.
  2. From the Internet Connection Type menu, select **Fixed**.

The screen adjusts:

The screenshot shows the IPv6 configuration interface. At the top, there are 'Cancel' and 'Apply' buttons. Below that, the 'Internet Connection Type' is set to 'Fixed'. The 'WAN Setup' section contains four rows of input fields: 'IPv6 Address/Prefix Length', 'Default IPv6 Gateway', 'Primary DNS Server', and 'Secondary DNS Server'. The 'LAN Setup' section has two radio buttons: 'Use DHCP Server' (unselected) and 'Auto Config' (selected). Below the radio buttons is another 'IPv6 Address/Prefix Length' field. At the bottom, the 'IPv6 Filtering' section has two radio buttons: 'Secured' (selected) and 'Open' (unselected).

3. Configure the fixed IPv6 addresses for the WAN connection:
  - **IPv6 Address/Prefix Length.** The IPv6 address and prefix length of the modem router WAN interface.
  - **Default IPv6 Gateway.** The IPv6 address of the default IPv6 gateway, which is supposed to be on the modem router's WAN interface.
  - **Primary DNS Server.** The primary DNS server that resolves IPv6 domain name records for the modem router.
  - **Secondary DNS Server.** The secondary DNS server that resolves IPv6 domain name records for the modem router.

**Note:** *If you do not specify the DNS servers, the modem router uses the DNS servers that are configured for the IPv4 Internet connection on the Internet Setup screen. (For more information, see [Internet Setup](#) on page 24.)*

4. Specify how the modem router assigns IPv6 addresses to the devices on your home network (the LAN) by selecting one of the following radio buttons:
  - **Use DHCP Server.** This method passes more information to LAN devices, but some IPv6 systems might not support the DHCPv6 client function.
  - **Auto Config.** This is the default setting.
5. In the IPv6 Address/Prefix Length fields, specify the static IPv6 address and prefix length of the modem router's LAN interface.

If you do not specify an ID here, the modem router generates the address and prefix length automatically from its MAC address.

6. Specify the IPv6 filtering mode by selecting one of the following radio buttons:
  - **Secured.** In the secured mode, which is the default mode, the modem router inspects both TCP and UDP packets.
  - **Open.** In the open mode, the modem router inspects UDP packets only.
7. Click the **Apply** button.

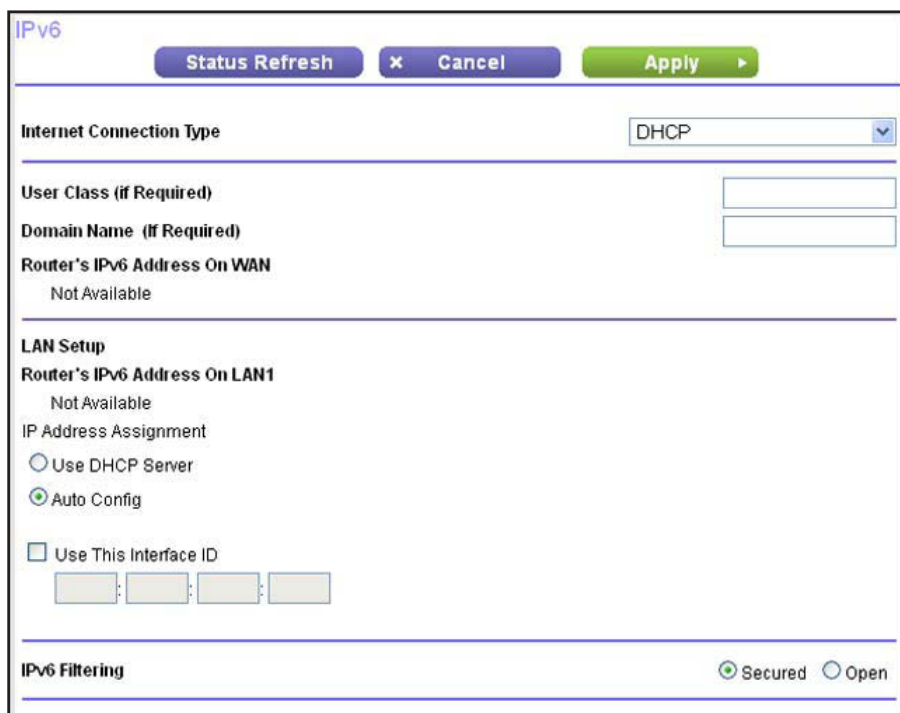
Your settings are saved.

## IPv6 DHCP

➤ **To set up an IPv6 Internet connection with a DHCP server:**

1. Select **ADVANCED > Advanced Setup > IPv6**.
2. From the Internet Connection Type menu, select **DHCP**.

The screen adjusts:



The modem router automatically detects the information in the following fields:

- **Router's IPv6 Address on WAN.** This field shows the IPv6 address that is acquired for the modem router's WAN (or Internet) interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline ( ) under the IPv6 address. If no address is acquired, the field displays Not Available.
- **Router's IPv6 Address on LAN1.** This field shows the IPv6 address that is acquired for the modem router's LAN interface. The number after the slash (/) is the length of

the prefix, which is also indicated by the underline (   ) under the IPv6 address. If no address is acquired, the field displays Not Available.

3. (Optional) In the User Class (If Required) field, enter a host name.

If your ISP has given you a specific host name, enter it here. Otherwise, leave this field blank.

4. (Optional) In the Domain Name (If Required) field, enter a domain name.

You can type the domain name of your IPv6 ISP. (Do not enter the domain name for the IPv4 ISP here.) For example, if your ISP's mail server is mail.xxx.yyy.zzz, type xxx.yyy.zzz as the domain name.

If your ISP provided a specific domain name, type it in this field. (For example, Earthlink Cable might require a host name of home, and Comcast sometimes supplies a domain name.)

5. Specify how the modem router assigns IPv6 addresses to the devices on your home network (the LAN) by selecting one of the following radio buttons:
  - **Use DHCP Server.** This method passes more information to LAN devices, but some IPv6 systems might not support the DHCPv6 client function.
  - **Auto Config.** This is the default setting.
6. (Optional) Select the **Use This Interface ID** check box, and specify the interface ID that you want to be used for the IPv6 address of the modem router's LAN interface.

If you do not specify an ID here, the modem router generates one automatically from its MAC address.

7. Specify the IPv6 filtering mode by selecting one of the following radio buttons:
  - **Secured.** In the secured mode, which is the default mode, the modem router inspects both TCP and UDP packets.
  - **Open.** In the open mode, the modem router inspects UDP packets only.
8. Click the **Apply** button.

Your settings are saved.

## IPv6 PPPoE

### ➤ To set up a PPPoE IPv6 Internet connection:

1. Select **ADVANCED > Advanced Setup > IPv6**.
2. From the Internet Connection Type menu, select **PPPoE (PPP over Ethernet)**.

The screen adjusts:

The screenshot shows the IPv6 configuration page. At the top, there are three buttons: "Status Refresh", "Cancel", and "Apply". Below the buttons, the "Internet Connection Type" is set to "PPPoE(PPP over Ethernet)". There are three input fields for "Login", "Password", and "Service Name (If Required)". The "Connection Mode" is set to "Always On". The "Router's IPv6 Address On WAN" field displays "Not Available". Under the "LAN Setup" section, the "Router's IPv6 Address On LAN1" field also displays "Not Available". The "IP Address Assignment" section has two radio buttons: "Use DHCP Server" and "Auto Config", with "Auto Config" selected. There is a checkbox for "Use This Interface ID" which is currently unchecked, followed by four empty input boxes. At the bottom, the "IPv6 Filtering" section has two radio buttons: "Secured" (selected) and "Open".

The modem router automatically detects the information in the following fields:

- **Router's IPv6 Address on WAN.** This field shows the IPv6 address that is acquired for the modem router's WAN (or Internet) interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline ( \_ ) under the IPv6 address. If no address is acquired, the field displays Not Available.
  - **Router's IPv6 Address on LAN1.** This field shows the IPv6 address that is acquired for the modem router's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline ( \_ ) under the IPv6 address. If no address is acquired, the field displays Not Available.
3. In the Login field, enter the login information for the ISP connection.  
This is usually the name that you use in your email address. For example, if your main mail account is JerAB@ISP.com, type JerAB in this field. Some ISPs (such as Mindspring, Earthlink, and T-DSL) require that you use your full email address when you log in. If your ISP requires your full email address, type it in this field.
  4. In the Password field, enter the password for the ISP connection.
  5. In the Service Name (If Required) field, enter a service name.  
If your ISP did not provide a service name, leave this field blank.

**Note:** *The default setting of the Connection Mode field is Always On to provide a steady IPv6 connection. The modem router never terminates the connection. If the connection is terminated, for example, when the modem is turned off, the modem router attempts to reestablish the connection immediately after the PPPoE connection becomes available again.*

6. Specify how the modem router assigns IPv6 addresses to the devices on your home network (the LAN) by selecting one of the following radio buttons:
  - **Use DHCP Server.** This method passes more information to LAN devices, but some IPv6 systems might not support the DHCPv6 client function.
  - **Auto Config.** This is the default setting.
7. (Optional) Select the **Use This Interface ID** check box, and specify the interface ID that you want to be used for the IPv6 address of the modem router's LAN interface.

If you do not specify an ID here, the modem router generates one automatically from its MAC address.
8. Specify the IPv6 filtering mode by selecting one of the following radio buttons:
  - **Secured.** In the secured mode, which is the default mode, the modem router inspects both TCP and UDP packets.
  - **Open.** In the open mode, the modem router inspects UDP packets only.
9. Click the **Apply** button.

Your settings are saved.

## Traffic Meter

Traffic metering allows you to monitor the volume of Internet traffic that passes through the modem router Internet port. With the traffic meter utility, you can set limits for traffic volume, set a monthly limit, and get a live update of traffic usage.

➤ **To monitor Internet traffic:**

1. Click **ADVANCED > Advanced Setup > Traffic Meter**.

**Traffic Meter** Cancel Apply

---

**Internet Traffic Meter**

Enable Traffic Meter

Traffic volume control by No limit

Monthly limit 0 Mbytes

Round up data volume for each connection by 0 Mbytes

Connection time control

Monthly limit 0 hours

---

**Traffic Counter**

Restart traffic counter at  :  am On the  day of each month

Restart Counter Now

---

**Traffic Control**

Pop up a warning message

Mbytes/Minutes before the monthly limit is reached

When the monthly limit is reached

Turn the Internet LED to flashing green/amber

Disconnect and disable the Internet connection

---

**Internet Traffic Statistics**

Start Date/Time: Tuesday Jan 1 00:00:00 2013  
 Current Date/Time: Tuesday Jan 1 00:00:41 2013  
 Traffic Volume Left: 0

Counting Period	Connection Time (hh:mm)	Traffic Volume (Mbytes)		
		Upload/Avg	Download/Avg	Total/Avg
Today	0:0	0.00	0.00	0.00
Yesterday	0:0	0.00	0.00	0.00
This week	0:0	0.00/0.00	0.00/0.00	0.00/0.00
This month	0:0	0.00/0.00	0.00/0.00	0.00/0.00
Last month	0:0	0.00/0.00	0.00/0.00	0.00/0.00

Refresh Traffic Status

2. Select the **Enable Traffic Meter** check box.

By default, there is no traffic limit and the traffic volume is not controlled.

3. In the Traffic Counter section, set the traffic counter to begin at a specific time and date.
4. (Optional) If you want the traffic counter to start immediately, click the **Restart Counter Now** button.
5. Click the **Apply** button.

Your settings are saved.

The Internet Traffic Statistics section helps you to monitor the data traffic.

➤ **To update the Traffic Statistics section:**

Click the **Refresh** button.

- **To display more information about the data traffic on your modem router and to change the poll interval:**

Click the **Traffic Status** button.

## Restricting Internet Traffic by Volume

You can record and restrict the traffic by volume in MB. This is useful when your ISP measures your traffic in volume.

- **To record and restrict the volume of Internet traffic by volume:**

1. Click **ADVANCED > Advanced Setup > Traffic Meter**.

The Traffic Meter screen displays.

2. Select the **Enable Traffic Meter** check box.
3. Select the **Traffic volume control by** radio button.
4. From the menu, select one of the following options for controlling the traffic volume:
  - **Download only.** The restriction is applied to incoming traffic only:
  - **Both Directions.** The restriction is applied to both incoming and outgoing traffic:
5. In the Monthly Limit field, enter how many MBytes (MB) per month are allowed.
6. If your ISP charges you an amount of extra data volume when you make a new connection, enter the extra data volume in MB in the Round up data volume for each connection by field.
7. (Optional) In the Traffic Control section, enter a value in MB to specify when the modem router issues a warning message before the monthly limit in volume is reached.

The modem router issues a warning when the balance falls under the volume that you enter. By default, the value is 0 and no warning message is issued.

8. (Optional) Select one or both of the following actions to occur when the limit is reached:
  - Select the **Turn the Internet LED to flashing green/amber** check box.

When the traffic limit is reached, the Internet LED alternates blinking green and amber.

- Select the **Disconnect and disable the Internet connection** check box.

When the traffic limit is reached, the Internet connection is disconnected and disabled.

9. Click the **Apply** button.

Your settings are saved.



## Restricting Internet Traffic by Connection Time

You can record and restrict the traffic in connection time. This is useful when your ISP measures your connection time.

➤ **To record and restrict the volume of Internet traffic by volume:**

1. Click **ADVANCED > Advanced Setup > Traffic Meter**.

The Traffic Meter screen displays.

2. Select the **Enable Traffic Meter** check box.
3. Select the **Connection time control** radio button.
4. In the Monthly Limit field, enter how many hours per month are allowed.
5. (Optional) In the Traffic Control section, enter a value in minutes to specify when the modem router issues a warning message before the monthly limit in hours is reached.

The modem router issues a warning when the balance falls under the minutes that you enter. By default, the value is 0 and no warning message is issued.

6. (Optional) Select one or both of the following actions to occur when the limit is reached:

- Select the **Turn the Internet LED to flashing green/amber** check box.

When the traffic limit is reached, the Internet LED alternates blinking green and amber.

- Select the **Disconnect and disable the Internet connection** check box.

When the traffic limit is reached, the Internet connection is disconnected and disabled.

7. Click the **Apply** button.

Your settings are saved.

# 8 Troubleshooting

---

# 8

## Get help with problems

This chapter provides information to help you diagnose and solve problems you might have with your modem router. If you do not find the solution here, check the NETGEAR support site at <http://support.netgear.com> for product and contact information.

This chapter contains the following sections:

- *Quick Tips*
- *Troubleshoot with the LEDs*
- *Cannot Log In to the Modem Router*
- *Troubleshoot the Internet Connection*
- *Changes Not Saved*
- *Wireless Connectivity*
- *Incorrect Date or Time*
- *TCP/IP Network Not Responding*

## Quick Tips

This section describes tips for troubleshooting some common problems.

### Sequence to Restart Your Network

If you need to restart your network, follow this sequence:

1. Turn off and unplug the modem router.
2. Plug in the modem router and turn it on.

Wait two minutes.

### Check Ethernet Cable Connections

Make sure that the Ethernet cables are securely plugged in.

For each powered-on computer connected to the modem router by an Ethernet cable, the corresponding numbered LAN port LED on the modem router is on.

### Wireless Settings

Make sure that the wireless settings in the wireless computer and modem router match exactly.

- For a wirelessly connected computer, the wireless network name (SSID) and wireless security settings of the modem router and wireless computer must match exactly.
- If you set up an access list on the Advanced Wireless Settings screen, you must add each wireless computer's MAC address to the modem router's access list.




### Network Settings

Make sure that the network settings of the computer are correct.


- Wired and wirelessly connected computers must have network (IP) addresses on the same network as the modem router. The easiest way to do this is to use computers that obtain an IP address automatically with DHCP. Most computers are set up this way.
- Some cable modem service providers require you to use the MAC address of the computer initially registered on the account. You can view the MAC address on the Attached Devices screen.

## Troubleshoot with the LEDs

When you turn on the power, the Power, LAN, and DSL LEDs light as described here. If they do not, refer to the sections that follow for help.

1. When power is first applied, the Power LED lights solid red.
2. After approximately 10 seconds, the LAN port LED lights green  for any local ports that are connected.
3. After approximately 1 minute, the DSL link LED lights green  to indicate that a DSL link is established.
4. After approximately one minute, the Power LED turns solid green .

### Power LED Is Off

If the Power  and other LEDs are off when your modem router is turned on:

- Check that the On/Off button on the back panel is in the On position, that is, it is pushed in.
- Check that the power cord is correctly connected to your modem router and that the power supply adapter is correctly connected to a functioning power outlet.
- Check that you are using the 12 VDC 1A power adapter supplied by NETGEAR for this product.

If the error persists, you might have a hardware problem. For recovery instructions, or help with a hardware problem, contact technical support at [www.netgear.com/support](http://www.netgear.com/support).

### Power LED Is Red

When the modem router is turned on, it performs a power-on self-test, during which time the Power LED turns red. If the Power LED does not turn green within a minute or so, or if it turns red at any other time during normal operation, there is a fault within the modem router.

If the Power LED turns red to indicate a modem router fault, turn the power off and on to see if the modem router recovers. If the Power LED is still red one minute after power-up:

- Turn the power off and on one more time to see if the modem router recovers.
- Clear the modem router's configuration to factory defaults (see *Side Panel with Restore Factory Settings Button* on page 12). This sets the modem router's IP address to 192.168.0.1.


If the error persists, you have a hardware problem. For recovery instructions, or help with a hardware problem, contact technical support at [www.netgear.com/support](http://www.netgear.com/support).

## Power LED Is Blinking


If the Power LED blinks slowly and continuously, the firmware of the modem router is corrupted. This can occur if a firmware update is interrupted, or if the modem router detects a problem with the firmware.

If the error persists, you have a hardware problem. For recovery instructions, or help with a hardware problem, contact technical support at [www.netgear.com/support](http://www.netgear.com/support).

## WiFi LED Is Off

If the WiFi LED  stays off, check to see if the WiFi On/Off button on the modem router has been pressed. This button turns the wireless radio in the modem router on and off. The WiFi LED lights when the wireless radio is turned on.

## LAN LED Is Off

If the LAN LED  for a port does not light when you connect a device, check the following:

- The Ethernet cable connections are secure at the modem router and at the hub or device.
- The power is turned on to the connected hub or device.
- You are using the correct cable.

## Cannot Log In to the Modem Router

If you are unable to log in to the modem router from a computer on your local network, check the following:


- If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the modem router (see the previous section).
- Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to be sure that the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure that you are using the correct login information. The factory default login name is **admin**, and the password is **password**. Make sure that Caps Lock is off when you enter this information.
- Make sure that your computer's IP address is on the same subnet as the modem router. If you are using the recommended addressing scheme, your computer's address must be in the range of 192.168.0.2 to 192.168.0.254.
- If your computer's IP address is shown as 169.254.x.x, recent versions of Windows and Mac OS generate and assign an IP address if the computer cannot reach a DHCP server. These autogenerated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the modem router, and reboot your computer.

- If your modem router's IP address was changed and you do not know the current IP address, clear the modem router's configuration to factory defaults. This sets the modem router's IP address to 192.168.0.1. This procedure is explained in *Side Panel with Restore Factory Settings Button* on page 12.


## Troubleshoot the Internet Connection

If your modem router is unable to access the Internet, check the ADSL connection, then the WAN TCP/IP connection.

### ADSL Link

If your modem router is unable to access the Internet, first determine whether you have a DSL link with the service provider. The state of this connection is indicated with the Internet LED .

#### DSL LED Is Green

If your DSL link LED  is green, you have a good ADSL connection. You can be confident that the service provider has connected your line correctly and that your wiring is correct.

#### DSL LED Is Blinking Green

If your DSL LED is blinking green, your modem router is attempting to make an ADSL connection with the service provider. The DSL LED turns green within several minutes.

If the DSL LED does not turn green, disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time, being sure to use a microfilter on each telephone. If the microfilters are connected correctly, you can connect all your telephones.

If disconnecting telephones does not result in a green DSL LED, there might be a problem with your wiring. If the telephone company has tested the ADSL signal at your network interface device (NID), then you might have poor-quality wiring in your house.

#### DSL LED Is Off or Internet LED is Off

If the DSL LED is off, Internet LED is off, or both are off, disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time, being sure to use a microfilter on each telephone. If the microfilters are connected correctly, you can connect all your telephones.

If disconnecting telephones does not result in a green DSL LED, check for the following:

- Check that the telephone company has made the connection to your line and tested it.
- Verify that you are connected to the correct telephone line. If you have more than one phone line, be sure that you are connected to the line with the ADSL service. It might be necessary to use a swapper if your ADSL signal is on pins 1 and 4 or the RJ-11 jack. The modem router uses pins 2 and 3.

## Internet LED Is Red

If the Internet LED is red, the device was unable to connect to the Internet. Verify the following:

- Check that your login credentials are correct, or that the information you entered on the Internet Setup screen is correct.
- Check if your ISP has a problem—it might not be that the modem router cannot connect to the Internet, but rather that your ISP that cannot provide an Internet connection.

## Obtaining an Internet IP Address

If your modem router is unable to access the Internet, and your Internet LED is green, see if the modem router can obtain an Internet IP address from the ISP. Unless you have been assigned a static IP address, your modem router requests an IP address from the ISP. You can determine whether the request was successful using the browser interface.

### ➤ To check the WAN IP address:

1. Launch your browser, and select an external site such as [www.netgear.com](http://www.netgear.com).
2. Access the main menu of the modem router's at <http://www.routerlogin.net>.
3. Select **Administration > Router Status**.
4. Check that an IP address is shown for the Internet port.

If 0.0.0.0 is shown, your modem router has not obtained an IP address from your ISP.

If your modem router is unable to obtain an IP address from the ISP, the problem might be one of the following:

- Your Internet service provider (ISP) might require a login program. Ask your ISP whether they require PPP over Ethernet (PPPoE) or some other type of login.
- If you have selected a login program, the service name, user name, or password might be incorrectly set. For more information, see the following section, [Troubleshoot PPPoE or PPPoA](#).
- Your ISP might check for your computer's host name. Assign the computer host name of your ISP account as the account name on the Internet Setup screen.
- Your ISP allows only one Ethernet MAC address to connect to Internet, and might check for your computer's MAC address. In this case, do one of the following:
  - Inform your ISP that you have bought a new network device, and ask them to use the modem router's MAC address.
  - Configure your modem router to clone your computer's MAC address. You can do this on the Internet Setup screen (see [Internet Setup](#) on page 24).

## Troubleshoot PPPoE or PPPoA

➤ **To verify if your PPPoE or PPPoA connection is working:**

1. Select **ADVANCED > Administration > Router Status**.  
The Router Status screen displays.
2. In the Modem pane, check the following:  
The Modem Status is connected.
3. In the Internet Port pane, check the following:
  - A valid IP address and subnet mask are displayed.
  - The connection is PPPoE or PPPoA.
4. In the Internet Port pane, click the **Connection Status** button.  
The Connection Status screen displays.
5. Check the following:
  - The Connection Status is connected.
  - The Connection Time is not zero (00:00:00).

If all of the information is correct, your PPPoE or PPPoA connection is working.

➤ **If your PPPoE or PPPoA connection does not function, attempt to reconnect:**

1. Select **ADVANCED > Administration > Router Status**.  
The Router Status screen displays.
2. In the Internet Port pane, click the **Connection Status** button.  
The Connection Status screen displays.
3. Click the **Connect** button.  
The modem router attempts to reconnect.

If you cannot connect after several minutes, you might be using an incorrect service name, user name, or password. There might also be a provisioning problem with your ISP.

Unless you connect manually, the modem router does not authenticate using PPPoE or PPPoA until data is transmitted to the network.

## Troubleshoot Internet Browsing

If your modem router can obtain an IP address, but your computer is unable to load any web pages from the Internet:

- Your computer might not recognize any DNS server addresses.

A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP provides the addresses of one or two DNS servers for your use. If you entered a DNS address when you set up the modem



router, reboot your computer, and verify the DNS address. Alternatively, you can configure your computer manually with DNS addresses, as explained in your operating system documentation.

- Your computer might not have the modem router configured as its TCP/IP modem router. If your computer obtains its information from the modem router by DHCP, reboot the computer, and verify the modem router address.

## Changes Not Saved

If the modem router does not save the changes you make in the modem router web management interface, check the following:

- When entering configuration settings, always click the **Apply** button before moving to another screen or tab, or your changes are lost.
- Click the **Refresh** or **Reload** button in the web browser. The changes might have occurred, but the old settings might be in the web browser's cache.

## Wireless Connectivity

If you are having trouble connecting wirelessly to the modem router, try to isolate the problem.

- Does the wireless device or computer that you are using find your wireless network?

If not, check the WiFi LED on the front of the modem router. If it is off, you can press the **WiFi On/Off** button on the front of the modem router to turn the modem router wireless radio back on.

If you disabled the modem router's SSID broadcast, your wireless network is hidden and does not display in your wireless client's scanning list. (By default, SSID broadcast is enabled.)

- Does your wireless device support the security that you are using for your wireless network (WPA or WPA2)?
- If you want to view the wireless settings for the modem router, use an Ethernet cable to connect a computer to a LAN port on the modem router. Then log in to the modem router, and select **Wireless** (see *Basic Wireless Settings* on page 36).

**Note:** *Be sure to click the **Apply** button if you change settings.*

If your wireless device finds your network, but the signal strength is weak, check these conditions:

- Is your modem router too far from your computer, or too close? Place your computer near the modem router, but at least 6 feet (1.8 meters) away, and see whether the signal strength improves.
- Are objects between the modem router and your computer blocking the wireless signal?

## Incorrect Date or Time

The modem router uses the Network Time Protocol (NTP) to obtain the current time from one of several network time servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include the following:

- Date shown is January 1, 2003. This means the modem router has not yet reached a network time server. Check that your Internet access is configured correctly. If you have just finished setting up the modem router, wait at least five minutes, and check the date and time again.
- Time is off by one hour. The modem router has an automatic daylight saving time setting.

➤ **To change the modem router setting for daylight saving time:**

1. Select **Security > Schedule**.
2. Select the **Automatically adjust for daylight savings time** check box.
3. Click the **Apply** button.

Your changes are saved.

## TCP/IP Network Not Responding

Most TCP/IP terminal devices and routers have a ping utility for sending an echo request packet to the designated device. The device responds with an echo reply to tell whether a TCP/IP network is responding to requests.

### Test the LAN Path to Your Modem Router

You can ping the modem router from your computer to verify that the LAN path to your modem router is set up correctly.

➤ **To ping the modem router from a Windows computer:**

1. From the Windows taskbar, click the **Start** button, and select **Run**.
2. In the field provided, type **ping** followed by the IP address of the modem router, as in this example:

**ping 192.168.0.1**

3. Click the **OK** button.

A message such as the following one displays:

Pinging <IP address> with 32 bytes of data

If the path is working, you see this message:

Reply from < IP address >: bytes=32 time=NN ms TTL=xxx

If the path is not working, you see this message:

```
Request timed out
```

If the path is not functioning correctly, you might have one of the following problems:

- Wrong physical connections

For a wired connection, make sure that the numbered LAN port LED is lit for the port to which you are connected.

- Wrong network configuration
  - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer or workstation.
  - Verify that the IP address for your modem router and your workstation are correct and that the addresses are on the same subnet.

## Test the Path from Your Computer to a Remote Device

After you verify that the LAN path works correctly, test the path from your computer to a remote device:

1. From the Windows toolbar, click the **Start** button and select **Run**.
2. In the Windows Run screen, type:

```
ping -n 10 IP address
```

where *IP address* is the IP address of a remote device such as your ISP's DNS server.

If the path is functioning correctly, replies as described in [Test the LAN Path to Your Modem Router](#) on page 146 display. If you do not receive replies:

- Check that your computer has the IP address of your modem router listed as the default modem router. If the IP configuration of your computer is assigned by DHCP, this information is not visible in your computer's Network Control Panel. Verify that the IP address of the modem router is listed as the default router.
- Check that the network address of your computer (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- If your ISP assigned a host name to your computer, enter that host name as the account name on the Internet Setup screen (see [Internet Setup](#) on page 24).
- Your ISP might be rejecting the Ethernet MAC addresses of all but one of your computers.

Many broadband ISPs restrict access by allowing traffic only from the MAC address of your modem, but some additionally restrict access to the MAC address of a single computer connected to that modem. In this case, configure your modem router to clone or spoof the MAC address from the authorized computer.

## A Supplemental Information

---



View the factory settings and specifications

This appendix includes the factory default settings and technical specifications for the modem router.

This appendix contains the following sections:

- *Factory Settings*
- *Technical and Physical Specifications*

## Factory Settings

You can return the modem router to its factory settings. On the right side panel of the modem router, use the end of a paper clip or some other similar object to press and hold the **Restore Factory Settings** button for at least seven seconds. (For more information about the location of the button, see *Side Panel with Restore Factory Settings Button* on page 12.) The modem router returns to the factory settings shown in the following table.

**Table 3. Factory default settings**

Feature		Default Behavior
Router Login	User login URL	www.routerlogin.com or www.routerlogin.net
	User name (case-sensitive)	admin
	Login password (case-sensitive)	password
Internet connection	WAN MAC address	Use default address
	WAN MTU size	1492
	Port speed	AutoSensing
Local network (LAN)	LAN IP	192.168.0.1
	Subnet mask	255.255.255.0
	RIP direction	None
	RIP version	Disabled
	RIP authentication	None
	DHCP server	Enabled
	DHCP starting IP address	192.168.0.2
	DHCP ending IP address	192.168.0.254
	DMZ	Enabled or disabled
	Time zone	GMT for WW except GR, GMT+1 for GR, GMT-8 for NA
	Time zone adjusted for daylight savings time	Disabled
	SNMP	Disabled
Firewall	Inbound (communications coming in from the Internet)	Disabled (except traffic on port 80, the HTTP port)
	Outbound (communications going out to the Internet)	Enabled (all)
	Source MAC filtering	Disabled

**Table 3. Factory default settings (continued)**

Feature		Default Behavior
Wireless	Wireless communication	Enabled
	SSID name	See the label on the modem router.
	Security	See the label on the modem router.
	Broadcast SSID	Enabled
	Country/region	Varies by region
	RF channel	Auto
	Operating mode	Up to 65 Mbps
	Data rate	Best
	Output power	Full
	Access point	Enabled
	Authentication type	Pre-shared Key
	Wireless card access list	All wireless stations allowed

## Technical and Physical Specifications

**Table 4. Technical and physical specifications**

Specification	Description
Network protocol and standards compatibility	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE or PPPoA, RFC 1483 Bridged or Routed Ethernet, and RFC 1577 Classical IP over ATM
Power adapter	North America: 120V, 60 Hz, input
	UK, Australia: 240V, 50 Hz, input
	Europe: 230V, 50 Hz, input
	All regions (output): 12V @ 1A output
Physical	Dimensions: 186 x 135 x 60 mm (7.32 x 5.31 x 2.36 in)
	Weight: 270.8 g (0.597 lb)
Environmental	Operating temperature: 0° to 40°C (32° to 104°F)
	Operating humidity: 10% to 90% relative humidity, noncondensing
	Storage temperature: -20° to 70°C (-4° to 158°F)
	Storage humidity: 5 to 95% relative humidity, noncondensing
Regulatory compliance	EN 55 022 (CISPR 22), Class B
LAN interface specifications	10BASE-T or 100BASE-Tx, RJ-45
WAN interface specifications	One ADSL RJ-11 port (with pins 2 and 3) with support for: <ul style="list-style-type: none"> <li>• T1.413, G.DMT, G.Lite</li> <li>• ITU Annex A hardware or Annex B hardware</li> <li>• ITU G.992.5 (ADSL2+)</li> </ul>

# B Notification of Compliance

---



## NETGEAR wireless routers, gateways, APs

### Regulatory Compliance Information

This section includes user requirements for operating this product in accordance with National laws for usage of radio spectrum and operation of radio devices. Failure of the end-user to comply with the applicable requirements may result in unlawful operation and adverse action against the end-user by the applicable National regulatory authority.

This product's firmware limits operation to only the channels allowed in a particular Region or Country. Therefore, all options described in this user's guide may not be available in your version of the product.

### Europe – EU Declaration of Conformity

Products bearing the **CE** marking comply with the following EU directives:

- EMC Directive 2004/108/EC
- Low Voltage Directive 2006/95/EC

If this product has telecommunications functionality, it also complies with the requirements of the following EU Directive:

- R&TTE Directive 1999/5/EC

Compliance with these directives implies conformity to harmonized European standards that are noted in the EU Declaration of Conformity.

For indoor use only. Valid in all EU member states, EFTA states, and Switzerland.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 - 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

### FCC Requirements for Operation in the United States

#### FCC Information to User

This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals.

#### FCC Guidelines for Human Exposure

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

#### FCC Declaration of Conformity

We, NETGEAR, Inc., 350 East Plumeria Drive, San Jose, CA 95134, declare under our sole responsibility that the N150 Wireless ADSL2+ Modem Router DGN1000Bv3 complies with Part 15 Subpart B of FCC CFR47 Rules.

Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.



## FCC Radio Frequency Interference Warnings & Instructions

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an electrical outlet on a circuit different from that which the radio receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

## FCC Caution

- Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
- This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
- For product available in the USA and Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.
- Pour les produits disponibles aux États-Unis / Canada du marché, seul le canal 1 à 11 peuvent être exploités. Sélection d'autres canaux n'est pas possible.
- This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.
- Cet appareil et son antenne (s) ne doit pas être co-localisés ou fonctionnement en association avec une autre antenne ou transmetteur.

## TV Tuner (on Selected Models)

Note to CATV System Installer: This reminder is provided to call the CATV system installer's attention to Section 820-93 of the National Electrical Code, which provides guidelines for proper grounding and, in particular, specifies that the Coaxial cable shield be connected to the grounding system of the building as close to the point of cable entry as possible.

## Canadian Department of Communications Radio Interference Regulations

This digital apparatus (N150 Wireless ADSL2+ Modem Router DGN1000Bv3) does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

This Class [B] digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe [B] est conforme à la norme NMB-003 du Canada

## Industry Canada

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

## Caution:

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

**IMPORTANT NOTE: Radiation Exposure Statement:**

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

**NOTE IMPORTANTE: Déclaration d'exposition aux radiations:**

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

**Interference Reduction Table**

The table below shows the recommended minimum distance between NETGEAR equipment and household appliances to reduce interference (in feet and meters).

Household Appliance	Recommended Minimum Distance (in feet and meters)
Microwave ovens	30 feet / 9 meters
Baby monitor - analog	20 feet / 6 meters
Baby monitor - digital	40 feet / 12 meters
Cordless phone - analog	20 feet / 6 meters
Cordless phone - digital	30 feet / 9 meters
Bluetooth devices	20 feet / 6 meters
ZigBee	20 feet / 6 meters